Dell Security Management Server

Technical Advisories v10.2.11

June 2020
Rev. A01

Notes, cautions, and warnings

NOTE: A NOTE indicates important information that helps you make better use of your product.

CAUTION: A CAUTION indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.

WARNING: A WARNING indicates a potential for property damage, personal injury, or death.

Contents

Chapter 1: Dell Security Management Server Technical Advisories..... 6
Contact Dell ProSupport..... 6
New Features and Functionality v10.2.11..... 6
Resolved Technical Advisories v10.2.11..... 6
Technical Advisories v10.2.11..... 7
New Features and Functionality v10.2.10..... 7
Resolved Technical Advisories v10.2.10..... 8
Technical Advisories v10.2.10..... 9
New Features and Functionality v10.2.9..... 10
Resolved Technical Advisories v10.2.9..... 10
Technical Advisories v10.2.9..... 10
New Features and Functionality v10.2.7..... 10
Resolved Technical Advisories v10.2.7..... 12
Technical Advisories v10.2.7..... 12
New Features and Functionality v10.2.6..... 12
Resolved Technical Advisories v10.2.6..... 12
Technical Advisories v10.2.6..... 12
New Features and Functionality v10.2.5..... 13
Resolved Technical Advisories v10.2.5..... 13
Technical Advisories v10.2.5..... 13
New Features and Functionality v10.2.4..... 13
Resolved Technical Advisories v10.2.4..... 13
Technical Advisories v10.2.4..... 13
New Features and Functionality v10.2.3..... 13
Resolved Technical Advisories v10.2.3..... 14
Technical Advisories v10.2.3..... 14
New Features and Functionality v10.2.2..... 14
Resolved Technical Advisories v10.2.2..... 14
Technical Advisories v10.2.2..... 14
New Features and Functionality v10.2.1..... 15
Resolved Technical Advisories v10.2.1..... 15
Technical Advisories v10.2.1..... 15
New Features and Functionality v10.1..... 15
Resolved Technical Advisories v10.1..... 15
Technical Advisories v10.1..... 16
New Features and Functionality v10.0..... 16
Resolved Technical Advisories v10.0..... 16
Technical Advisories v10.0..... 16
New Features and Functionality v9.11..... 16
Resolved Technical Advisories v9.11..... 17
Technical Advisories v9.11..... 17
New Features and Functionality v9.10..... 17
Resolved Technical Advisories v9.10..... 17
Technical Advisories v9.10..... 18
New Features and Functionality v9.9..... 18

Resolved Technical Advisories v9.9....18
Technical Advisories v9.9....19
New Features and Functionality v9.8....19
Resolved Technical Advisories v9.8....19
Technical Advisories v9.8....21
New Features and Functionality v9.7....22
Resolved Technical Advisories v9.7....22
Technical Advisories v9.7....23
New Features and Functionality v9.6....23
Resolved Technical Advisories v9.6....23
Technical Advisories v9.6....24
New Features and Functionality v9.5....24
Resolved Technical Advisories v9.5....25
Technical Advisories v9.5....25
New Features and Functionality v9.4.1.6....26
New Features and Functionality v9.4.1....26
Resolved Technical Advisories v9.4.1....26
New Features and Functionality v9.4....26
Resolved Technical Advisories v9.4....26
Technical Advisories v9.4....27
New Features and Functionality v9.2....28
Resolved Technical Advisories v9.2....28
Technical Advisories v9.2....29
New Features and Functionality v9.1.5....29
Resolved Technical Advisories v9.1.5....30
Technical Advisories v9.1.5....30
New Features and Functionality v9.1....30
Resolved Technical Advisories v9.1....30
Technical Advisories v9.1....31
New Features and Functionality v9.0....31
Resolved Technical Advisories v9.0....31
Technical Advisories v9.0....32
Resolved Technical Advisories v8.5.1....32
Technical Advisories v8.5.1....32
New Features and Functionality v8.5....33
Resolved Technical Advisories v8.5....33
New Features and Functionality v8.3.1....33
Resolved Technical Advisories v8.3.1....33
New Features and Functionality v8.3....34
Resolved Technical Advisories v8.3....34
Technical Advisories v8.3....34
New Features and Functionality v8.1....35
Resolved Technical Advisories v8.1....35
Technical Advisories v8.1....35
New Features and Functionality v8.0....35
Resolved Technical Advisories v8.0....35
Resolved Technical Advisories v7.7.2....36
Technical Advisories v7.7.2....36
New Features and Functionality v7.7.1....36
Resolved Technical Advisories v7.7.1....36

Technical Advisories v7.7.1 36
New Features and Functionality v7.7 36
Technical Advisories v7.2.3 37
Technical Advisories v7.2.1 37
Technical Advisories v7.2 37
Technical Advisories v7.0/7.0.1 37

Chapter 2: Default Policy Changes 38

1

Dell Security Management Server Technical Advisories

Contact Dell ProSupport

Call 877-459-7304, extension 4310039 for 24x7 phone support for your Dell product.

Additionally, online support for Dell products is available at dell.com/support. Online support includes drivers, manuals, technical advisories, FAQs, and emerging issues.

Be sure to help us quickly connect you to the right technical expert by having your Service Tag or Express Service Code available when you call.

For phone numbers outside of the United States, see Dell ProSupport International Phone Numbers.

New Features and Functionality v10.2.11

- SQL Server 2019 is now supported.
- Microsoft Edge is now supported.
- The Security Management Server may have issues with UI elements for Internet Explorer 11. Due to the lack of support for modern web engines, Internet Explorer 11 will no longer be supported.
- The Security Management Server is compatible with the Microsoft requirement for LDAP channel binding and LDAP signing when Active Directory is in use.

  To enable this requirement on the Security Management Server, you must have the root issuing certificate for the domain controller certificates that are imported into the "Trusted Root" store within the Microsoft Certificate Key Store.
- Licenses purchased on-the-box can now be bulk-inserted with a .csv file. To obtain this file, contact your Dell Security sales representative or Dell Security support.
- The Security Server service now automatically adds the Server local IP addresses to ipWhitelist on service startup.
- Management Console:
  - For **Management > Commit Policies**, the embedded help now also includes content for *View Pending Commit(s)*.
  - On the Endpoints page, the PBE and Manager columns are no longer included as part of the endpoint information. An *Enabled Technologies* column now displays all the plugins that are enabled on the endpoint.
  - The EMS Device Whitelist field now accepts a maximum of 150 characters per line and 500 lines.

Resolved Technical Advisories v10.2.11

- The Encryption recovery file that is downloaded from the Security Management Server is no longer wrapped inside an executable file and does not require running a command to extract it. [DDPS-5054]
- The APNS (Apple Push Notification Server) database tables, which are used for iOS device support, have been removed. [DDPS-9453]
- The MDM (mobile device support) database tables have been removed. [DDPS-9454]
- When sending an email through JavaMail in the **Management Console > Notification Management** page, the Console sends the email as anonymous. Updating to the latest version of JavaMail resolved the issue. [DDPS-9494]
- The password used when downloading an endpoint recovery bundle is no longer written in cleartext in output.log file from the Security Server logs when in debug mode. [DDPS-9541]
- In the **Management Console > Notification Management** page, the *Send Test Email* dialog now displays the correct information. [DDPS-9542]
- Due to product deprecation, the `cloud-profile-updater. properties` file has been removed from `'/opt/dell/server/security-server/conf'` and `'/opt/dell/server/security-server/bin'`. [DDPS-9544]
- In the **Management Console > User Groups**, when an administrator tries to grant to a group a higher administrator role than the administrator account itself possesses, an *Access Denied* message displays rather than an *Internal Error* message. [DDPS-9548]

- When updating a Security Management Server's certificate using the **Advanced Configuration > Server Certificates > Create and Install Self-Signed Certificate** option, the system updates the *signingcertificate* table as expected.[DDPS-9549]
- If the Management Console times out and cannot connect to the Security Management Server, a more descriptive *Connection Refused* dialog now displays. Clicking **OK** redirects the user to the login page. [DDPS-9557]
- In the **Security Management Server > DMZ Server Support** field, the Host Name field now accepts any valid FQDN or hostname including those that begin with a number. [DDPS-9561, DDPS-9561]
- Threat Events are now sortable within an individual Endpoint. [DDPS-9568]
- Selecting the option to Bypass for an Endpoint Group now appropriately displays a confirmation dialog. [DDPS-9596]
- An issue where the Effective Policy for an Endpoint or a User would not properly update has been resolved. [DDPS-9621]
- An issue where the Encryption Failure View was not loading within the Security Management Server has been resolved. [DDPS-9622]
- Administrators with the Security Administrator role can now properly Remove and Add Endpoints to Groups within the Security Management Server. [DDPS-9626]
- The Threat Protection Status widget on the Dashboard now properly displays the color indicator per Threat Category. [DDPS-9634]
- The Device ID now links to the endpoint within the *Threat Events* tab. [DDPS-9640]
- When connecting to the Cylance server in the **Management Console > Advanced Threats** tab, a wait message no longer displays. [DDPS-9650]
- In the **Management Console > Management > Services Management > Events Management**, an issue has been resolved where the Security Server logs displayed recent events but would not export events when an unexpectedly older event was discovered. [DDPS-9662]
- Administrators with the Help Desk role can no longer remove endpoints that are presented within an endpoint's *Details and Actions* tab. [DDPS-9698]
- Advanced Threat Events once again can search by hostname or SHA256 hash. [DDPS-9710]

Resolved Security Advisories v10.2.11

- Several Java-based vulnerabilities have been resolved. [DDPS-9101, DDPS-9332]

  Updates are to these versions:

  - Java Version: 1.8.0.241
  - Jetty Version: 9.4.25
-

Technical Advisories v10.2.11

- In the Management Console, if endpoints display without Serial Number, the administrator must set the following:

  - `UseBiosSerialNumber` entries within the InventoryObjects.config (in Core Server for Encryption Enterprise; in Core Server and Inventory Server for Virtual Edition)
  - DeviceInventoryQueueProcessor
  - AgentInventoryQueueProcess

  The client and the agent must then update to use the *AssetTag* field instead of the *Serial* field that is stored in `DeviceData:UseBiosSerialNumber` entries. [DDPS-9619]
- Log Analyzer does not have the ability to filter using a start and end time. [DDPS-9637]
- Report emails scheduled through the **Management Console > Reporting > Manage Reports** feature do not localize the email subject properly for Japanese and Korean languages. [DDPS-9643]
- Currently, the **Uncommitted Policy Changes** notification displays to administrators whose roles do not have permission to commit policy. If they try to commit the outstanding policies, these administrators are logged out of the Management Console. [DDPS-9702]
- In the Management Console, MDM databases have been removed. Therefore, the Endpoints page lists an error: `Exception thrown in webservice controller java.lang.RuntimeException: NOT IMPLEMENTED: MDM_DEVICE`. Currently, this issue will not be fixed. [DDPS-9729]

New Features and Functionality v10.2.10

- The Security Management Server is improved through various security fixes and enhancements. See Resolved Security Advisories v10.2.10 for additional information.
- LDAP query responses are hardened in the Security Management Server.
- The Security Management Server is now signed by a SHA256 signing certificate as the SHA1 signing certificate is deprecated
- The Sync Users at PBA Activation policy is now enabled by default.

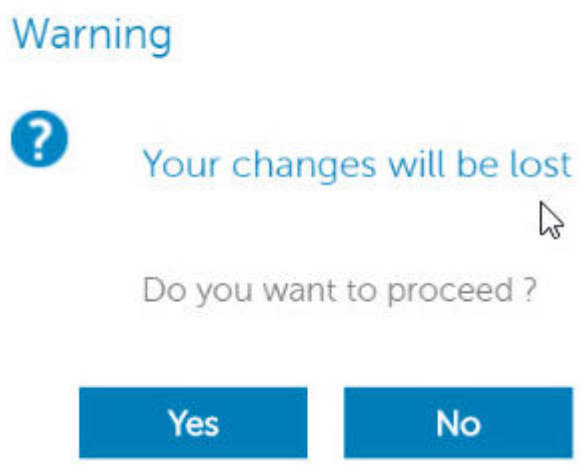
- The Security Management Server is now built with InstallShield 2019.
- The Security Management Server v10.2.10 now supports VMware ESXi 6.7
- *First Seen in System* and *Last Seen in System* columns have been added to **Populations > Endpoints > Details and Actions** for each disk in the selected endpoint.
- When communicating to the Cylance SaaS, delays in communication are presented with the following message:

  Attempting to connect to Cylance at this time. Please Check back in a bit.
- On upgrade, all users are reconciled by the Security Management Server to ensure all groups and users are accurately reflected in the Management Console.
- The now attempts to clean up the audit database by default and adheres to 80% of the 10 GB assigned database size. This cleaning action prevents critical errors displaying in the *Dashboard Notifications* pane, which previously detailed that the Audit Database exceeded its 95% size limitation.

  The **auditdb.size.NotificationPercentage** property is now included in**Application.properties** of the Security Server to manage the size of the Advanced Threat Prevention Audit database.

  The **auditdb.size.percentage** property is the cleanup threshold. When this percentage of the database is exceeded, after the **auditdb.clear.cron** is activated, the percentage of total space is calculated. The **auditdb.clear.cron** default value is every two hours.

  If the **auditdb.size.NotificationPercentage** value is exceeded, a notification of the cleanup displays the Security Management Server and the duration defined in **auditdb.cleanup.delete.hours** is used to clean up the data in the ddp_audit database below the **auditdb.size.percentage** threshold.
- After upgrading the Security Management Server, the following fields display the current date rather than Null:
  - Shield Activation
  - PBA Authentication
  - WebUI Login
  - User Creation in WebUI
  - Policy Proxy Sync
- When moving from one page to another, the following prompt displays if policy changes have not been saved.



Resolved Technical Advisories v10.2.10

- All instances of Data Guardian are removed from the *License Management* page. [DDPS-9367]
- The Management Console's *About* page now properly displays *Disconnected Mode* when Disconnected Mode is in use. [DDPS-9369]
- PBA Device Control commands now function as expected. [DDPS-9373]
- The Management Console now times out as expected after 30 minutes of inactivity. [DDPS-9387]
- Windows Port Control now properly displays a green check mark on the Security Policy tab when enabled. [DDPS-9397]
- User privileges are now properly evaluated after any modification to membership in Active Directory. [DDPS-9401, DDPSUS-2689, DDPSUS-2702]
- The sorting function on the *Dashboard Notifications* now behaves as expected. [DDPS-9405]
- Notifications can now be dismissed as expected. [DDPS-9406]
- Removing a device from an Endpoint Group no longer results in a javascript:null webpage. [DDPS-9421]

- When the Dell PostgresSQL service is inaccessible, the following message displays:

  Cannot reach the database, please ensure the Dell PostgresSQL Service is started. [DDPS-9462]
- The *Third Party* page now properly displays all third party information. [DDPS-9476]
- BitLocker Manager's Details Report now correctly displays drive letters. [DDPS-9496, DDPSUS-2714]
- Policy Logs in the *Commit* page now return valid date and time information in Log Analyzer when using a non-English browser language. [DDPS-9514]
- Users with Administrator privileges can now create Endpoint Groups and devices can be added or removed in the *Members* pane in the Management Console as expected. [DDPS-9515]
- The Security Management Server can now be configured to allow non-domain activations. If your environment requires this activation workflow, see KB article SLN306341. [DDPS-9531, DDPSUS-2578]

Resolved Security Advisories v10.2.10

- An issue allowing remote deserialization of data through an RMI interface is resolved. For more information, see KB article SLN320536. [DDPS-9446]
- An issue resulting in users with the Account Administrator role in the Security Management Server elevating their permissions inappropriately is resolved. [DDPS-9516]
- An issue resulting in blank headers incorrectly displaying during a security scan is resolved. [DDPS-9519]

Technical Advisories v10.2.10

- In rare circumstances, unaccepted policies do not display an error. As a work around, check the Security Server logs for Invalid Values. [DDPS-9501, DDPS-9534]
- If the common name of a user is changed at the Domain Controller level, the Management Console does not reflect the new name. [DDPS-9510]
- If an existing email notification is modified then saved, the next new email notification inherits the previous notification's modifications. [DDPS-9527]
- Non-domain activations using the same hostname and username previously activated against a Security Management Server fail to activate and log the following failure in the Compatibility Server.
  `Illegal activation attempt of non-domain User`[DDPS-9531, DDPSUS-2578]
- The **Refresh** button is not available in the Management Console on the following pages:
  - Domains
  - User Groups
  - User
  - Endpoint Groups
  - Endpoint Details and Actions

  As a work around, refresh the browser. [DDPS-9532]
- After the initial activation of Advanced Threat Prevention in the Management Console, the *Advanced Threat Details* page does not properly display. As a work around, log out and back into the Management Console. [DDPS-9533]
- When recreating the self-signed certificates for the Security Management Server Virtual, the Dell Manager policy signing certificate is not recreated. As a work around, import a certificate based on a previously created certificate (see KB article SLN302996 for more information). Alternatively, select **import an existing certificate** and choose **server.p12** for the Certificate then **server.key** for the private key. The default password for this key is `changeit`. [DDPS-9549]
- The Threat Events tab within Enterprise and per Endpoint can not currently be sorted. [DDPS-9568]
- When modifying the priority list for either Endpoint Groups or User Groups, attempting to sort by Priority in the edit phase results in an internal error message displayeding and the sort does not aupdate. Cancel the operation or refresh the page to return to the Group page. As a work around, do not sort while editing the priority list. [DDPS-9567]
- The *Uncommitted Policies* banner may persist after committing existing policy changes in the Management Console if using Internet Explorer 11 or earlier. [DDPS-9571]

Technical Security Advisories v10.2.10

- No security advisories exist.

New Features and Functionality v10.2.9

- Data Guardian is removed from the Management Console in the Security Management Server. To reference the latest documentation and Technical Advisories for Data Guardian, see dell.com/support or contact Dell ProSupport.
- Policy changes can now be viewed In Management > Commit by selecting **View Logs**. **View Logs** displays an overview of policy changes associated with the selected commit.
- New installs of the Security Management Server now listen on TLS 1.2 by default for all Java-based services, including Dell Security Server, Dell Device Server, and Dell Compliance Reporter Server. Note that the Dell Core Server is not configured by default to use TLS 1.2 on new installs to avoid introducing compatibility issues with other applications that may exist on the same server.

  Upgrading the Security Management Server does not change these by default to avoid any compatibility issues with currently connecting devices. For information on modifying the SSL/TLS accepted protocols for existing Security Management Server installs, and for information on securing the Dell Core server, a Microsoft .NET based service, see KB article SLN313386.

Resolved Technical Advisories v10.2.9

- Removing override prompts for pending policy changes now displays the correct number of changes under Uncommitted Policies. [DDPS-3974]
- The correct error message now displays when adding a domain with an invalid port number. [DDPS-6263]
- In License Management, the correct tooltip now displays when the license pool is exceeded. [DDPS-7176]
- All text now displays properly when adding or modifying Endpoint Groups or User Groups. [DDPS-7177]
- The German and French Event Managements page now properly displays. [DDPS-7249]
- Editing administrator roles in the Management Console now yields an accurate warning message. [DDPS-7300, DDPSUS-2311]
- Threat Protection licenses are now properly consumed when products are installed and deactivated. [DDPS-8925, DDPSUS-2590]
- An issue resulting in a column in Endpoint Groups not displaying is resolved. [DDPS-8832]
- Password validation no longer fails with an error if an administrator's password contains double quotations. [DDPS-8936]
- When installing the Security Management Server on Windows, the ACL service starts as expected if the administrator's password contains a backslash. [DDPS-8938]
- An issue resulting in failed certificate imports to the Security Server is resolved. [DDPS-8939]
- An issue resulting in truncated databases after an upgrade failure is resolved. [DDPS-8940]
- The Management Console now displays the correct number of protected endpoints on the Dashboard page and Endpoints page. [DDPS-8868]
- The Security Management Server installer now calculates the space required for the Postgres Audit database on the system drive. [DDPS-9059]
- An issue resulting in Digicert root not being imported after upgrading the Security Management Server is resolved. [DDPS-9246]
- In Manage Reports > Email Report Schedules, the page title now displays properly. [DDPS-9275]
- An issue caused by an incorrectly defined syslog/SIEM server in Events Management in the Management console which resulted in a loop in the Audit Event export job and excessive CPU usage is resolved. [DDPS-9307]
- An issue resulting in the *Bypass Login* command being incorrectly defined as the *Unlock* command for devices with a Pre-boot Authentication environment is resolved. [DDPS-9308]
- Encryption Technology now properly displays in the Device Detail pane when a specific endpoint is selected. [DDPS-9310]
- Modifications to syslog configuration in Services Management > Event Management is now logged in Security Server logs and Administrator Action logs as expected. [DDPS-9329]
- Advanced Threat Event Data now exports at the Endpoint level as expected. [DDPS-9327, DDPSUS-2658]

Technical Advisories v10.2.9

- No technical advisories exist.

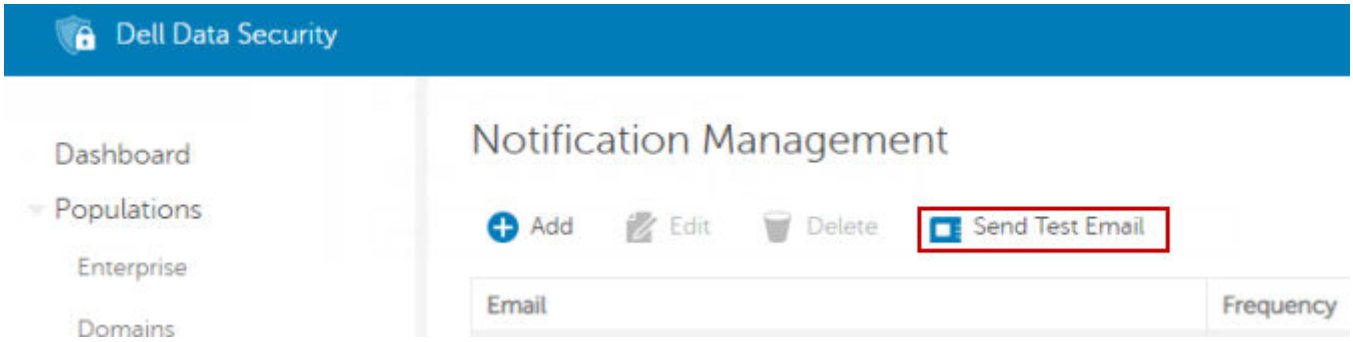
New Features and Functionality v10.2.7

- In Populations > Endpoint Groups, groups now display by policy priority.
- Endpoint groups have a new option to build groups based on a TPM being Present or a TPM being Active on a device with Dell Encryption installed.
- Test emails can now be sent in the Management Console to validate email workflows.

  To test the email workflow:

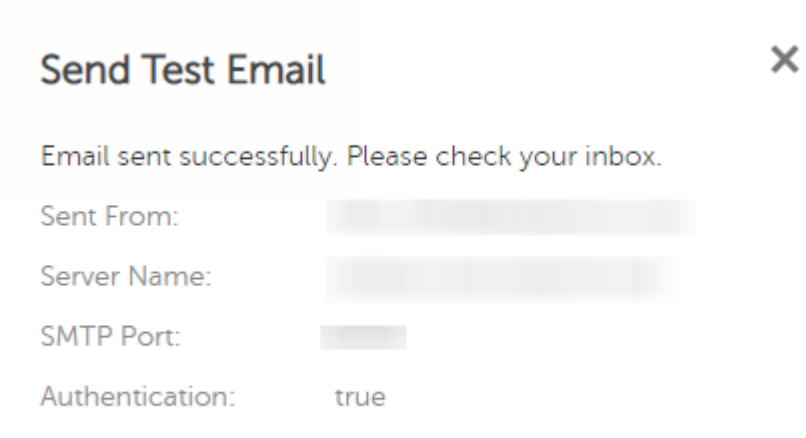
  1. Navigate to **Management > Notification Management**.

2. Select **Send Test Email**.

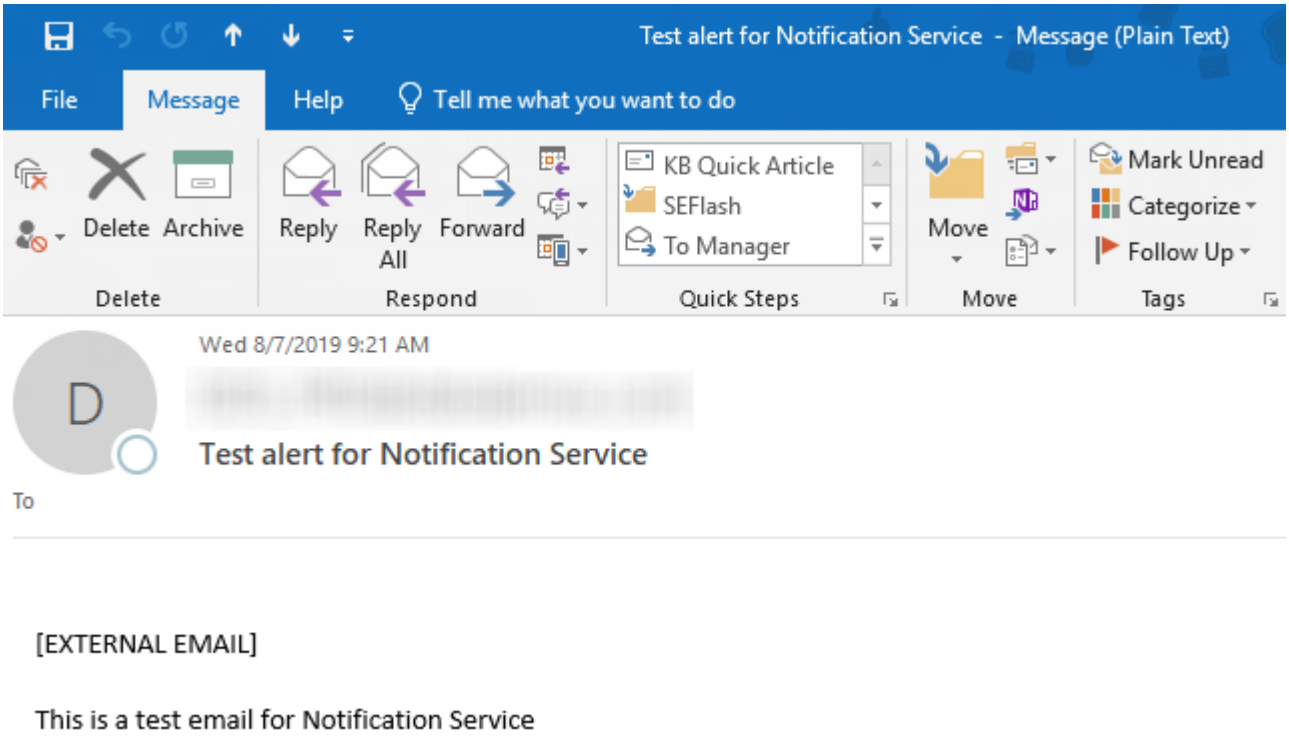


3. Specify the email to test and select **Send Email**.

If the email passes through the Dell Server successfully, the following results screen displays.



The following is an example of successful test email.



- The Data Guardian web portal can now be activated through a Security Management Server front end server. See Data Guardian Windows, Mac, Mobile, and Web Administrator Guide for requirements of activating the Data Guardian web portal against a Security Management Server.

Resolved Technical Advisories v10.2.7

- An issue resulting in the inability to log into the Data Guardian web portal is resolved. [DDPS-7310, DDPSUS-2557]
- The Server Configuration Tool now updates all required elements when importing SSL and TLS certificates. [DDPS-8450]
- Authentication processes around the Dell Server's message broker is improved. [DDPS-8456]
- Services are hardened to improve security posture. [DDPS-8487, DDPS-8689, DDPS-8740]
- An issue resulting in an inaccurate number of policy overrides displaying is resolved. [DDPS-8492]
- When changing priority values for Content Based Protection, all values populate and remain as expected. [DDPS-8531]
- Data Guardian users in an Access Group can now open swept files as expected when the Allow Access for Swept Files policy is enabled in the Dell Server. [DDPS-8556]
- Selected mobile devices can be removed from Populations > Endpoints as expected. [DDPS-8853]
- In Populations > Endpoints, Export File as an Excel document now functions as expected. [DDPS-8857]
- New email notifications no longer inherit modifications to existing email notifications. [DDPS-8881]
- Scheduled reporting emails now send at their scheduled time. [DDPS-8888]
- Manage Reports now only accepts emails distinguished by comma separated values. [DDPS-8955]

Technical Advisories v10.2.7

- Dell Data Guardian's Data Classification policy is rebranded to Content Based Protection. [DDPS-8855, DDPS-8861]
- The Postgres Audit database is now installed in C:\ProgramData. The Security Management Server installer currently does not calculate the space required for the Postgres Audit database on the system drive. [DDPS-9059]

New Features and Functionality v10.2.6

- The Dell ACL service is rebranded to Del Access Group service.

Resolved Technical Advisories v10.2.6

- The Security Management Server's built-in help file is now appropriate automatically translated for all supported languages based on browser locale. [DDPS-8566]
- Logs are now properly updated on the Log Analyzer page after adding a Web Portal URL on the Data Guardian Management page. [DDPS-8706]
- The Security Management Server's applications and resource files are now signed by Dell's SHA-1 and SHA-256 code-signing certificates. [DDPS-8711, DDPS-8712, DDPS-8722, DDPS-8723]
- User Groups and Endpoint Groups no longer accept special characters in the Priority field when using Internet Explorer. [DDPS-8735]
- Fields can be searched as expected in Managed Reports. [DDPS-8737]
- Type and Priority values are now retained after updating the Email field in Edit Notifications. [DDPS-8755]
- In Dashboard > Endpoint Protection Status > Protection Status, the Data Guardian column now displays as expected. [DDPS-8772]

Technical Advisories v10.2.6

- Selected mobile devices cannot currently be removed from Populations > Endpoints. As a work around, select the mobile device's hostname then select **Remove** on the Endpoint Details page. [DDPS-8853]
- In Populations > Endpoints, Export File as an Excel document fails with a 404 error. [DDPS-8857]
- In Dashboard > Endpoint Protection Status > Protection Status, the Shield column is rebranded to PBE. [DDPS-8771]
- Cloud Device Control commands do not currently generate logs. [DDPS-8866]
- If an existing email notification is modified then saved, the next new email notification inherits the previous notification's modifications. [DDPS-8881]
- Scheduled reporting emails send 30 minutes later than their scheduled time. [DDPS-8888]
- If an administrator's password contains double quotations, password validation fails and the following message displays:

  Credentials are invalid. Please verify the logon and password. [DDPS-8936]

- When installing the Security Management Server on Windows, if the administrator's password contains a backslash, the ACL service fails to start resulting in a timeout. [DDPS-8938]

New Features and Functionality v10.2.5

- No new features or functionality exist.

Resolved Technical Advisories v10.2.5

- Search performance for Advanced Threat Events and Audit Event data has been improved. [DDPS-8342, DDPS-8373]
- The default version of PostgreSQL has been updated to resolve third-party vulnerabilities. The PostgreSQL service leveraged by the Security Management Server is rebranded to Dell PostgreSQL 10.7. [DDPS-8480, DDPS-8985]
- An error is no longer returned to an external user when attempting to pre-share key access to another external user. [DDPS-8664]

Technical Advisories v10.2.5

- Logs are not properly updated on the Log Analyzer page after adding a Web Portal URL on the Data Guardian Management page. [DDPS-8706]
- When using Internet Explorer and editing priority, User Groups and Endpoint Groups incorrectly accepts special characters in the Priority field. [DDPS-8735]
- Type and Priority values are not retained after updating the Email field in Edit Notifications. [DDPS-8755]

New Features and Functionality v10.2.4

- A new policy can now be committed after changing the Portal URL.

  To update the portal URL:

  1. In the left pane, navigate to **Management > Data Guardian Management**.
  2. Select the **Web Portal** tab.
  3. Enter the updated URL and click **Save**.

  NOTE: The *Commit Policies* badge updates after the user navigates away from this page.
- Windows Server 2019 (Standard/Datacenter) is now supported.
- Circles of Trust is rebranded to Access Groups.

Resolved Technical Advisories v10.2.4

- Updated 6/2019 - Report Administrator, Report Owner, and Report User roles can now log in to the Management Console as expected. [DDPS-6101, DDPS-8625]
- An issue resulting in the *Type* and *Priority* fields persisting after creating multiple notifications in the Management Console is resolved. [DDPS-6779]
- Resolved an issue with malformed dates causing SIEM/Syslog events to improperly output to their network or local destinations. [DDPS-7570, DDPSUS-2325]
- An issue resulting in Managed Reports not displaying EMS events is resolved. [DDPS-8561, DDPSUS- 2532]
- An issue resulting in users with appropriate file rights not displaying in the Pre-Share UI is resolved. [DDPS-8567]
- Resolved an issue where the Security Management Server's Core Server, ACL Service, and Key Server would not start after a reboot. For more information, see https://www.dell.com/support/article/us/en/04/sln316840. [DDPS-8522]

Technical Advisories v10.2.4

- No technical advisories exist.

New Features and Functionality v10.2.3

- Administrators can now manage keys in the Management Console.

To find/change the owner for a key:

1. In the left pane, navigate to **Management > Data Guardian Management**.
2. Select the **Key Management** tab.
3. Enter the keyid and click **Find Owner**. The owner displays in the **Current Owner** field.
4. In the **New Owner** field, enter the email address of the new owner and click **Change Owner**.

To change ownership for all keys:

1. In the left pane, navigate to **Management > Data Guardian Management**.
2. Select the **Key Management** tab.
3. Select **Change Ownership for ALL keys**.
4. Enter the email address of the current owner.
5. Enter the email address of the new owner.
6. Click **Change Owner**.

During the transfer, a table displays at the bottom, *Key Changes in Progress*. When complete, this content is removed. The Log Analyzer displays a log of the keys that have changed ownership.

- Access Groups is now available the Management Console. To enable Access Groups:

1. In the left pane, navigate to **Management > Services Management**.
2. Select the **Data Guardian** tab.
3. For Access Groups, click **On**.

   For more information on Access Groups, refer to AdminHelp, available in the Management Console.

Resolved Technical Advisories v10.2.3

- An issue resulting in the PostGRESQL database not properly cleaning data during default configured cleanup jobs is resolved. After installation, on subsequent cleanup jobs, all previous jobs are reconciled. [DDPS-8397]
- An issue with data exported to a Syslog or SIEM server through Event Management in the Management Console is resolved. [DDPS-8398]

Technical Advisories v10.2.3

- In rare circumstances, pre-sharing a protected document with an embargo set may not in all cases pre-share the key. To work around this issue, manually share the key through the right-click menu from an internal user or an internal file owner. [DDPS-8567]

New Features and Functionality v10.2.2

- No new features or functionality exist.

Resolved Technical Advisories v10.2.2

- The Security Management Server now validates the version of Microsoft Visual C++ 2013 version 12.0.40660. If this version is not found, the installer exits. Please validate this version is installed before installing the Security Management Server. [DDPS-8010, DDPSUS-2437]
- Translation consistency is improved. [DDPS-8064]
- An issue resulting in service account names being rejected when starting with an escape character such as u and some special characters is resolved. [DDPS-8109]
- Clean installs of the Security Management Server no longer result in ACL service error messages. [DDPS-8149, DDPS-8270]
- Sorting by Classification Path in Audit Events no longer results in an error. [DDPS-8151]
- An issue that resulted in internal errors when transitioning between screens in the Management Console is resolved. [DDPS-8279]

Technical Advisories v10.2.2

- No technical advisories exist.

New Features and Functionality v10.2.1

- Audit data for blocked print screen events, blocked processes events, and blocked prints events are now displayed in the Management Console.

Resolved Technical Advisories v10.2.1

- Threat Events tab is now visible when at least one Threat Prevention or Advanced Threat Prevention license is consumed. [DDPS-5728]
- Manage Reports work as expected when special characters are added to the *Report Name* . [DDPS-6362]
- The default setting exclusions for weak ciphers are now preserved when upgrading from v9.10 to the latest Dell Security Management Server. [DDPS-7301]
- Time stamps used for "Commit" date/times are stored as UTC and will be converted to the current time-zone based on the time-zone setting of the system viewing the WebUI. [DDPS-7855]
- Resolved mismatching information for the *Unique ID* for endpoints on the "Endpoint" page, and on the "Device Detail" page. [DDPS-7928]
- Resolved an issue with dependency management, resulting in failures to update the Dell Security Management Server Virtual. [DDPS-7980]
- Resolved an issue with innocuous error messages within the Dell Beacon Service by removing unnecessary dependencies. [DDPS-7981]
- Resolved an incorrect symbolic link that resulted in additional storage overhead for logging. [DDPS-7991]
- Resolved an issue where the Windows Application for Dell Security Management Server may timeout or take an extremely long time to download key data. [DDPS-8121, DDPSUS-1796]

Technical Advisories v10.2.1

- No technical advisories exist.

New Features and Functionality v10.1

- A Downloads page has been added to Management Console for downloading Dell Data Security endpoint software.
- Scheduling report emails is now supported. A report must be created under Reporting > Manage Reports in the Management Console before the scheduling option is available.
    - The *Email* field is limited to 1024 characters.
    - *Day of Month* drop down will provide 1 - 31 and Last options to choose.
    - *Time*, will schedule the time based upon your current location.
    - Schedule Details page shows the date sent, schedule, next send, etc.

Resolved Technical Advisories v10.1

- A forensic key bundle download using the Administrative Download Utility (CMGAd) now succeed for endpoints with large key sets based on a high number of activations. [DDPS-6920, DDPSUS-2361]
- An issue resulting with a customer unable to run Advanced Threat Prevention reports while using the compliance reporter due to low memory has been resolved. [DDPS-7386, DDPSUS-2341]
- Dell Enterprise Server v10.1 includes a security update addressing a Jetty Security Bypass vulnerability (CVE-2017-7658). Customers and field teams should take v10.1 and all Dell Enterprise Server updates or sustaining releases as a best practice. [DDPS-7387, DDPSUS-2344]
- Selections made in the Audit Events page are now saved after a user navigates away from the page. [DDPS-7445]
- Servers with large amount of events from Advanced Threat Prevention may experience high memory usage on the Dell Security Management Server or Dell Security Management Server Virtual. This may result in services crashing on the server. Maximum heap space and physical memory can be increased to work-around this issue. [DDPS-7469]
- Compliance Reporter is hidden by default on the Management Console. [DDPS-7717]
- The email audit event under Data Guardian's Advanced Details for open events correctly shows the sender email in From. [DDPCE-9846]

Technical Advisories v10.1

- By default the Dell Security Management Server and Dell Security Center consoles will export data in UTF-8 format. In some cases, this data does not display properly if the file is opened and displayed in Unicode, which is done by default for Microsoft Excel. For information on opening files with UTF-8 encoding, see: https://support.office.com/en-us/article/choose-text-encoding-when-you-open-and-save-files-60d59c21-88b5-4006-831c-d536d42fd861?ocmsassetID=HA010121249&CorrelationId=050891fd-c54e-4e23-9e74-c8c75962d07f&ui=en-US&rs=en-US&ad=US. [DDPS-7613]
- When the Security Management Server is configured within an IPv6 environment with no IPv4 support, notification registration fails due to a communications error. To work around this issue, enable IPv4 support in this environment. [DDPS-7655]
- Navigating to the *Enterprise* > *Advanced Threat Events* tab and selecting the Host Name from the list results in being directed to Endpoint Details & Actions, instead of the Advanced Threat Events tab. To work around this issue, click **Advanced Threat Events** from *Details & Actions*. [DDPS-7739]
- When a recently added user attempts to log in the WebUI with a special character "\" in the user name, the login is unsuccessful and results with an error message displaying "The username or password used is invalid." [DDPS-7768]

New Features and Functionality v10.0

- Advanced Threat Prevention provisioning into geographical data centers for the Government Cloud is now supported.
- Additional maintenance tasks have been introduced to reduce the overall disk space used.

Resolved Technical Advisories v10.0

- BitLocker recovery keys are now sorted by date. [DDPS-6496]
- Advanced Threat Events are not properly populated within the Dell Compliance Reporter. [DDPS-6695]
- Advanced Threat Prevention email alert configuration is properly maintained. [DDPS-6710]
- An issue resulting with an error message of "A data access error occurred" when accessing the Key Revocation tab from the external user management page with text in the search box has been resolved. [DDPS-6716]
- Emails now properly send at the scheduled time within the Dell Compliance Reporter. [DDPS-6770]
- Intermittent domain communication no longer results in users being removed from the Dell Security Management Server. [DDPS-6914]
- Resolved an issue with updates not correctly retaining the username for connections to audit event data. [DDPS-7036]
- Basic authentication is now functioning again within the Dell Security Management Server Virtual. [DDPS-7244]

Technical Advisories v10.0

- Audit Events with pins per object counts close to 500 cause the management console to become unresponsive for some time. To work around this issue, modify the search scope to reduce the count below 500 consolidated events. [DDPS-7430]

New Features and Functionality v9.11

- Below are the requirements for SQL permissions. The current user performing the installation and the services must have local administrator rights.

Type	Action	Scenario	SQL Privilege Required
Back end	Upgrade	By definition, upgrades already have DB and Login/User established	db_owner
Back end	Restore Install	Restore involves an existing DB and login.	db_owner
Back end	New Install	Use existing DB	db_owner
Back end	New Install	Create new DB	dbcreator, db_owner
Back end	New Install	Use existing login	db_owner
Back end	New Install	Create new login	securityadmin
Back end	Uninstall	NA	NA

Type	Action	Scenario	SQL Privilege Required
Proxy Front end	Any	NA	NA

Resolved Technical Advisories v9.11

- Added 08/2018- Dashboard notification of immediate threats now read "Advanced Threat Prevention". [DDPS-4995]
- Dell Security Management Server Virtual 9.11 is built with Workstation 10.x hardware compatibility. [DDPS-5085]
- Customer is now able to upgrade with a default non-standard JKS password when trying to do a server recovery. [DDPS-5854]
- Adding devices to an existing endpoint group no longer requires a policy change for the destination endpoint group [DDPS-6002]
- Endpoints screen now displays serial number based off the bios serial number WMI value. [DDPS-6161]
- ATP Widget is now displayed by default for Administrators who log in to the WebUI before ATP is provisioned . [DDPS-6268]
- An issue resulting when a user would decline the End User License Agreement while set to English, the language screen would not appear after a reboot to the machine has been resolved. [DDPS-6365]

Technical Advisories v9.11

- When a user double clicks the login button on the Dell Data Guardian Web Portal, the download page will open instead of the upload page. To work around this issue, open a new tab and navigate back to the primary web portal URL. [DDPS-6792]
- Added 11/2018 - When upgrading from v9.10 to the latest Dell Security Management Server, default setting exclusions for weak ciphers are lost. To disable weak ciphers, seehttps://www.dell.com/support/article/us/en/19/sln301519/how-to-disable-weak-ciphers-in-dell-security-management-server-and-virtual-server-dell-data-protection-enterprise-edition-and-virtual-edition?lang=en. [DDPS-7301]

New Features and Functionality v9.10

- The option to remove user sweeps from protected status calculation on the server has been added.

  To enable, the administrator must modify the InventoryObjects.config file which is located in < C:\Program Files\Dell\Enterprise Edition\Core Server\> by default.

  the section to change is :

  <object name="DeviceInventoryQueueProcessor" singleton="false" type="Credant.Inventory.Processor.DeviceInventoryQueueProcessor, Credant.Inventory.Processor" >

  <property name="EvaluateLastLoggedInUserForProtection" value="true"/>

  </object>

  Changing the "true" value to "false" (this is not case sensitive) will require a restart of the core server service. Once the service has restarted the user sweep values are not calculated into the protected status for the device.
- Data Guardian has added the policies for protected office documents :
  - **Block Print Screen**: disables the user's ability to take screen captures via the Windows Print Screen capability while a Protected Office Document is open
  - **Protected Office Document Process Protection**: A comma separated list of EXE's that will be blocked from running while a Protected Office Document is open
- Web Portal Policies and their tool tips are localized.

Resolved Technical Advisories v9.10

- The "Enable Digital Signature Check" box in the WebUI now blocks the user from adding any text. [DDPS-5857]
- An issue that resulted in an error message during installation of Security Management Server with TLS 1.0 and TLS 1.1 disabled on the target SQL has been resolved. [DDPS-5982]
- Added 7/2019 - Java is updated to resolve a Remote Code Execution vulnerability in RMI Serialization (CWE-502). [DDPS-6200, DDPSUS-2084]

Resolved Customer Issues

- The database console does not accept invalid characters such as " ' " or " / ", etc. [DDPS-6102]

Technical Advisories v9.10

- Security Management Server Virtual may crash when pulling a high volume of keys in a short time-span. [DDPS-6193]

New Features and Functionality v9.9

- Uncommitted changes are now displayed in badge icon in the top left of the Remote Management Console.
- Widgets are now available in the Dell Server. In the top right of the Dashboard, the following options can be added or removed with the Widgets menu:
  - Notifications
  - Protections Status
  - Threat
  - Protection History
  - Inventory History
  - Summary Statistics
- The encryption technology in use now displays in the Protection Status tab of the Endpoint Details and Actions page.
- The Dell Server now supports IPV6.
- A Policy column has been added to **Manage Reports > Log Analyzer** which displays administrator actions related to Policy.
- License Management now uses the following definitions for license usage:
  - **Overage** - Over license count maximum. Activation of new endpoints will fail. Re-activation of clients will fail. Existing clients will function normally.
  - **Warning** - License count nearing limit. Activation of new endpoints will persist until 105% of maximum. Consider purchasing additional licenses.
  - **OK** - No action needed. Activation of new endpoints will persist until 105% of maximum. [DDPS-2115]
- A new policy enables Advanced Threat Prevention to detect and address malicious payloads with the following options:
  - Ignore - No action is taken against identified memory violations.
  - Alert - Record the violation and report the incident to the Dell Server.
  - Block - Block the process call if an application attempts to call a memory violation process. The application that made the call is allowed to continue to run.
  - Terminate - Block the process call if an application attempts to call a memory violation process and terminate the application that made the call.
- The Dell Server now supports TLS 1.2.

Resolved Technical Advisories v9.9

- The IP Exclusions for the Web Protection field in the Remote Management Console now only accepts valid formats. [DDPS-2206]
- If browser cookies are not enabled, the message "Cookies must be enabled on your browser to use this application" now displays at logon to the Remote Management Console. [DDPS-2661]
- A notification for a successful bulletin pull will now appear for the first successful bulletin pull after a bulletin pull failure. [DDPS-4811]
- Precedence changes for Endpoint Groups and User Groups are now displayed in the Log Analyzer. [DDPS-5024]
- AdminHelp and Compliance Reporter Help have been updated with Administrator Roles changes. The System role is marked as being able to "Manage Data Guardian external user key requests". [DDPS-5392, DDPS-5562, DDPS-5563]
- Duplicate Data Guardian key revocation requests involving the same file and user are displayed correctly in the Remote Management Console Key Revocation table. [DDPS-5570]
- The Device ID on the Enterprise-level Threat Events tab is now hyperlinked to its Endpoint Detail page in the Remote Management Console. [DDPS-5571]
- Logs now display the group name of a removed Admin-Defined User Group in Log Analyzer in the Remote Management Console. Logs are now generated when an Admin-Defined Endpoint Group is modified. [DDPS-5564, DDPS-5565]
- When running Log Details in Compliance Reporter, logs now show Username details as expected. [DDPS-5584]
- Logs are now generated as expected when an Approve or Deny file access request is issued. [DDPS-5589]
- The error message that displays during installation on the Server 2016 when the prerequisite .Net 3.5 is not already installed correctly displays "Server 2016". [DDPS-5591]
- Endpoints can now be exported as expected in Excel or CSV format. [DDPS-5825, DDPS-5826]

Resolved Customer Issues

- An issue that resulted in the Advanced Threats tab failing to load is resolved. [DDPS-5025]

- Compliance Reporter now shows the hostname of endpoints activated with Opt-in parameters. [DDPS-5527]
- Encryption External Media reports now show user information. [DDPS-5576]
- Recovery keys now download as expected for a hostname containing Unicode. [DDPS-5614]
- The appropriate number of licenses are now consumed when Endpoint Security Suite Enterprise is installed with Client Firewall and Web Protection features. [DDPS-5673]
- Files exported as CSV from the Advanced Threat Events tab now display the correct time stamp. [DDPS-5732]
- When using an unauthenticated SMTP connection, the Server Configuration Tool no longer requires a username or password. [DDPS-5785]
- An issue has been resolved that resulted in an internal error when accented characters were entered in the commit field. [DDPS-5805]

Technical Advisories v9.9

- Added 02/2018- Upgrades to Dell Security Management Server 9.9.2 are now blocked for server versions prior to Dell Data Protection | Encryption Enterprise Server version 9.2. [DDPS-6254]
- During installation or upgrade of the Security Management Server, an active script is run in the %TEMP% directory, which may be blocked by antivirus. To work around this, Dell recommends disabling all antivirus solutions before installing or upgrading the Security Management Server. [DDPS-5832]
- When setting a Firewall Rule and defining an executable within that rule, the MD5 checksum value does not validate the syntax. Ensure that the MD5 entry is properly set before finalizing the addition of an executable. [DDPS-5858]

New Features and Functionality v9.8

- Security Management Server now supports the Data Guardian web client. Based on policy, internal and external users can view and edit protected Office documents and .xen files, with Print Control, Block Copy, and Embargo features, without installing the full Data Guardian client on their computers. The administrator runs a quick installation to set up a virtual machine that hosts the web client and communicates with the Dell Server.
- An administrator can revoke Data Guardian keys for individual files shared with an external user, on either the External User Management page or the Audit Events page, and can now blacklist an external user from the Audit Events page.
- Policy allows Data Guardian Windows and Mobile to apply an onscreen watermark to protected Office documents and PDFs. The watermark identifies the user and is displayed when the document is printed or shared.
- Advanced Threat Prevention and Data Guardian endpoints now show to have Protected status on the Endpoints page when their agents report their plugins' status as Functional. Plugin Status is displayed on the Providers tab of the Endpoint Details & Actions page.
- Advanced Threat Prevention audit events can now be exported to a SIEM/syslog server and to a local file from **Management** > **Services Management** in both connected and disconnected mode.
- Advanced Threat Event notification emails now include hyperlinks to additional detail about each category of event (Critical, High, Medium, Low, and Total).
- A new Web Protection policy allows administrators to block more than 100 specific categories of information.
- Administrators can now bulk upload and import a CSV list of Users to add to Admin-Defined User Groups. User Group priority can now be modified using drag-and-drop functionality.
- The License Management page now displays On the Box Licenses Collected, with the relevant Service Tags.
- Pre-Boot Authentication policies now display in the Authentication Technology Group on the Security Policies tab. A new policy allows the administrator to enable or disable users' ability to select **Remember Me** on the PBA login screen.
- As of v9.8, the ESXi vSphere thick client can no longer be used for deployment.
- The Remote Wipe command to remove a Dropbox for Business user has been deprecated. Administrators may use the Dropbox for Business function to remove users.
- Hardware Crypto Accelerator and Mobile Edition are no longer supported. Their policies have been deprecated.
- Enterprise Server is rebranded to Security Management Server.

Resolved Technical Advisories v9.8

- An error now displays when an invalid domain address is entered for DNS blocking in Threat Prevention Client Firewall settings. [DDPS-3201]
- Connection types are now validated; the executables table now displays the value entered for Signature and the correct column name for Fingerprint; and a network name is now required for specifying network protocol, when adding a Threat Prevention Client Firewall custom rule. EtherType and custom EtherType values (for non-IP network protocol) and transport protocol values display after a Firewall rule is saved. Duplicate rules must now be saved with unique rule names. [DDPS-3429, DDPS-3678, DDPS-3679, DDPS-3725, DDPS-3726, DDPS-3727, DDPS-5196]

- The administrator role change confirmation prompt now shows the correct user name after a user's administrative roles are modified, and the prompt now displays for changes made from the User Details Admin tab. [DDPS-4097, DDPS-4099]
- The error that displays when an invalid or blank hostname is entered during installation now displays the label of the field in the installer. [DDPS-4466]
- The diagnostic tool, Data Collection Utility, is now included in the Start menu with other Server components. [DDPS-4918]
- An external user no longer must reactivate Data Guardian after being removed from the Full Access List. [DDPS-5021]
- Log Analyzer logs are now generated when notification email addresses are added or edited in Notification Management. [DDPS-5063]
- Audit event exports to the SIEM/syslog server are now resent if a transmission error occurs during the initial export attempt. [DDPS-5132]
- Active Directory contacts' Data Guardian registration now succeeds, and the prompt for a domain password no longer displays during registration. [DDPS-5160, DDPS-5164, DDPS-5168]
- Formatting requirements for the following Advanced Threat Prevention policies are now included in Dell Server tooltips and AdminHelp: Memory Actions - Exclude executable files, Script Control - Approve Scripts in Folders (and Subfolders), and Protection Settings - Exclude Specific Folders (includes subfolders). AdminHelp now correctly indicates that the Help Desk and Security Administrator roles can download recovery key bundles. [DDPS-5184, DDPS-5287]
- Hyperlinks in Advanced Threat Prevention notifications now function properly when one or more endpoints are activated against a Dell Server with the host property set to the front-end Server host. [DDPS-5188]
- All files are now installed in the expected locations after upgrade on a Dell Server running in Disconnected Mode when previously installed files were stored in a non-default location. [DDPS-5190]
- The "Certificate" type is now populated in the Type of Notification column of the All Notification Report in Compliance Reporter. [DDPS-5217]
- Upgrade no longer fails when the Run As Service account is changed during the upgrade. [DDPS-5226]
- Audit events can be exported to a SIEM/syslog server with TLS/SSL over TCP, with the following configuration changes:

  To use TLS/SSL, the syslog server must be configured to listen for TLS/SSL messages. The root certificate used for the syslog server configuration must be added to the Dell Server Java keystore.

  The following example shows necessary configurations for a Splunk server with default certificates. Configurations are specific to individual environments. Property values vary when using non-default certificates.

  1. Configure the Splunk server to use the Splunk Server certificate and root certificate to listen on TCP for TLS/SSL messages:

     $SPLUNK_HOME\etc\system\local\inputs.conf

     [tcp-ssl:<port number>]

     disabled = 0

     [SSL]

     serverCert = $SPLUNK_HOME\etc\auth\server.pem

     sslPassword = <password>

     requireClientCert = false

     $SPLUNK_HOME\etc\system\local\server.conf

     [sslConfig]

     sslRootCAPath = $SPLUNK_HOME\etc\auth\cacert.pem

     sslPassword = <password>
  2. Restart the Splunk server.

     After the restart, **splunkd.log** will have entries similar to the following:

     07-10-2017 16:27:02.646 -0500 INFO TcpInputConfig - IPv4 port 5540 is reserved for raw input (SSL)

     07-10-2017 16:27:02.646 -0500 INFO TcpInputConfig - IPv4 port 5540 will negotiate new-s2s protocol

     07-10-2017 16:27:02.653 -0500 INFO TcpInputConfig - IPv4 port 5540 is reserved for raw input (SSL)

     07-10-2017 16:27:02.653 -0500 INFO TcpInputConfig - IPv4 port 5540 will negotiate new-s2s protocol

     07-10-2017 16:27:02.653 -0500 INFO TcpInputConfig - IPv4 port 9997 is reserved for splunk 2 splunk

     07-10-2017 16:27:02.653 -0500 INFO TcpInputConfig - IPv4 port 9997 will negotiate new-s2s protocol

     07-10-2017 16:27:02.653 -0500 INFO TcpInputProc - Creating raw Acceptor for IPv4 port 5540 with SSL

     07-10-2017 16:27:02.653 -0500 INFO TcpInputProc - Creating raw Acceptor for IPv4 port 5541 with Non-SSL

     07-10-2017 16:27:02.654 -0500 INFO TcpInputProc - Creating fwd data Acceptor for IPv4 port 9997 with Non-SSL

3. Configure the Dell Server to communicate with the Splunk server and export audit events.

   Use the keytool command to add the Splunk server's root certificate (cacert.pem) to the Dell Server operating system Java keystore. The certificate is added to the operating system Java keystore and not to the Dell Server application Java keystore.

   ```
   keytool -keystore <keystore_location> -alias <alias-name> -importcert -file
   <certificate_file>
   ```

   For Security Management Server - Add the Splunk server's root certificate (cacert.pem) to the Java keystore, which in Windows is usually located in this path: `C:\Program Files\Dell\Java Runtime\jre1.8\lib\security\cacerts`

   For Security Management Server Virtual - Add the Splunk server's root certificate (cacert.pem) to `/etc/ssl/certs/java/cacerts` and restart the Dell Server.

4. Modify the Dell Server database to change the SSL value from **false** to **true**.

   In the database, navigate to the information table, SIEM-specific support configuration.

   Change the "SSL":"false" value to "SSL":"true" - for example:

   ```
   {"eventsExport":{"exportToLocalFile":{"enabled":"false","fileLocation":"./logs/siem/audit-
   export.log"},"exportToSyslog":
   {"enabled":"true","protocol":"TCP","SSL":"true","host":"yourDellServer.yourdomain.com","por
   t":"5540"}}}
   ```

[DDPS-5234]

Resolved Customer Issues

- An issue is resolved that resulted in a license import failure with an error in the Security Server log that the system cannot find the `\AppData\Local\Temp\` folder. [DDPS-4240]
- Installation now proceeds as expected when the Service Runtime Account password that is used during installation contains "**$_**" (dollar sign followed by underscore). [DDPS-4923]
- Attempts to re-register a Data Guardian user that is already registered now fail with a messages that the user is already registered and confirmed. [DDPS-5133]
- An issue related with Microsoft platform validation profile changes that prevented BitLocker Manager from beginning to encrypt on Windows 10 is now resolved. [DDPS-5243]
- The Device Lease Period can now be reduced to a minimum of 14 days. [DDPS-5281]
- An issue that resulted in an access violation error in module 'GKConsole.exe' is now resolved. [DDPS-5300]
- A page selector and drop-down list now allows the administrator to navigate between pages of Endpoint Groups and select the number of groups to display per page. [DDPS-5349]
- Policy commit comments that begin with special characters are now logged in Commit History. [DDPS-5353]
- Certificates with passwords that include special characters can now be successfully imported. [DDPS-5396]
- The installer now accepts a period (".") in the SQL service account username with SQL Server 2008 R2 and SQL Server 2016. [DDPS-5418]
- Duplicate entries no longer display in the BitLocker Manager Detail report in Compliance Reporter after upgrade. [DDPS-5432]
- An issue is resolved with Threat Protection (TP) licenses for Web Protection and Firewall, and they now match consumed licenses for Advanced Threat Prevention (ATP) with Web Protection and Firewall. [DDPS-5491]

Technical Advisories v9.8

- Added 01/2018-Advanced Threat Event results are automatically limited to the first 10000 results. This will resolve issues where Advanced Threat Events were not properly displaying when selecting the tab within the Dell Security Management Server
- To block all PowerShell scripts with Advanced Threat Prevention, both the PowerShell and PowerShell Console policies must be set to **Block**. When both policies are set to Block, no scripts can be run, either through the PowerShell console or the Cmd console. PowerShell one-liners are blocked. To allow approved scripts to run through the Cmd console, select the Enable Approve Scripts in Folders (and Subfolders) policy, and add the approved scripts to the Approve Scripts in Folders (and Subfolders) policy. The PowerShell Console policy applies to PowerShell v3 and later. Windows 7 includes PowerShell v2, by default. To upgrade to PowerShell v3 on Windows 7, see www.microsoft.com/en-us/download/details.aspx?id=34595. [CYL-619]
- As of v9.8, the ESXi vSphere thick client can no longer be used for deployment. Also, previous installs on ESXi 5.1 have not been prevented although they are not supported. Installs on ESXi 5.1 are now prevented. [DDPS-5086, DDPS-5269]
- The Office Protected Files Cover Page Corporate Logo policy cannot be committed when running the Remote Management Console in Firefox. To work around this issue, use Internet Explorer or Google Chrome. [DDPS-5538]
- Added 08/2018-The Dell Policy Proxy service may incorrectly send two requests to the back end server for SKID3 requests. This can safely be ignored. [DDPS-5585]

New Features and Functionality v9.7

- Enterprise Server now supports Advanced Threat Prevention with optional Client Firewall and Web Protection features. Client Firewall and Web Protection policies are reorganized to simplify management of these features. Prior to client upgrade to the new features, refer to Default Policy Changes.
- Enterprise Server now supports Disconnected Mode, for air-gapped environments.
- Added 7/2017 - Enterprise Server is now supported with VMware ESXi 6.5.
- Active Directory groups and domains can now be specified when adding or modifying Endpoint Groups. Enterprise Server collects Active Directory information from endpoints and makes this data available for Endpoint Group specification.
- Endpoint Group Precedence can now be modified using drag-and-drop functionality. This functionality applies to Admin-Defined, Rule-Defined, and Active Directory but not System-Defined Endpoint Groups. Precedence of System-Defined Endpoint Groups for new installations and upgrades is as follows: Highest precedence is given to Non-Persistent VDI followed by Persistent VDI Endpoint Group. Lowest precedence is given to Default followed by Opt-in Endpoint Group.
- Added 7/2017 - Administrators can now bulk upload and import a CSV list of Endpoints to add to Admin-Defined Endpoint Groups.
- Advanced Threat Prevention and Dell Data Guardian events can now be exported to a syslog server or to a local file through a streamlined Events Management screen.
- New Advanced Threat Prevention policies allow Application Control folder exclusions and automatic deletion of quarantined files after a configurable length of time.
- Log Analyzer results can now be exported to Excel or CSV file.
- New Enterprise Edition for Mac policies replace the need to manage some settings through .plist entries.
- Secure Lifecycle is rebranded to Dell Data Guardian.

Resolved Technical Advisories v9.7

- On the Client Firewall Custom Rule Specify Network page in the Remote Management Console, the Fully qualified domain name field now validates and rejects invalid formats. Also, the Transport protocol drop-down list item **ICMP** and the displayed Message type are now consistent. [DDPS-2820, DDPS-2826, DDPS-2885]
- Transport Protocol values are now populated in the drop-down list in Client Firewall Custom Rules. [DDPS-3819].
- AdminHelp can now be moved to avoid obscuring important fields in the Remote Management Console. [DDPS-4258]
- A few Data Guardian External User Management items that were previously untranslated in the Remote Management Console are now translated. [DDPS-4404]
- The following Enterprise Port Control policies now display with Class: Storage, their parent policy: Subclass Storage: External Drive Control, Subclass Storage: Optical Drive Control, and Subclass Storage: Floppy Drive Control. [DDPS-4682]
- Added 08/2018- Administrators can log in to endpoints with the Logon Authentication Policy for Administrator policy set to **None** and **None**. [DDPS-4739]
- Filtering in the Remote Management Console Advanced Threats Protection tab is now functioning as expected. [DDPS-4772]
- The Error Validating Policy dialog that displays when an updated policy value fails validation now includes the related policy name. [DDPS-4812]
- The Data Guardian policy, Enable Callback Beacon, is now disabled by default. [DDPS-4985]
- Advanced Threat Event Dashboard Notifications are now properly categorized by Type. [DDPS-4994]
- Localizations of Remote Management Console are improved.

Resolved Customer Issues

- Recovery of an EMS-encrypted device now proceeds as expected on a computer and Dell Server other than the original encrypting computer and Server originally managing the device encryption, when the Servers belong to the same federation. To configure federation, follow these steps:

  1. On one of the Servers to be federated, edit `<installation folder>\Enterprise Edition\Security Server \conf\federatedservers.properties`:

     server.code - Replace "ENC(<Server code>)" with "CLR(<new code; string of characters you select>)". This will be a shared code among the federated Servers.

     Server.uris - List the Servers to be federated, separated with commas. Example: https://server1:8443,https://server2:8443
  2. Save federatedservers.properties.
  3. Copy federatedservers.properties and save it off the Security Server.

     NOTE: The file must be saved off the Security Server before restart.
  4. Restart the Security Server.

After restart, "CLR(<new code; string of characters you select>)" is changed to "ENC(<new shared code>)" and the new shared Server code is applied to the Security Server.

5. Copy the federatedservers.properties file to the `\Security Server\conf` folder of each Server to be federated.
6. Restart each Security Server after copying federatedservers.properties to its \conf folder.

[DDPS-2889]

- An issue is resolved that resulted in an intermittent Internal Error in the Remote Management Console. [DDPS-4446]
- SSL/TLS protocols for Compliance Reporter are now configurable in the eserver.ssl.protocols property in the `reporter/conf/eserver.properties` file and are preserved during backup/restore operations. [DDPS-4547]
- An issue is resolved in the French Remote Management Console that resulted in an internal error when accessing the Dashboard. [DDPS-4675]
- A single alias can now be used for more than one domain, allowing filtering for users across the different domains. [DDPS-4683]
- The Spanish translation of the policy override success message is corrected. [DDPS-4718]
- Importing a certificate during installation now proceeds as expected when spaces exist in the certificate alias. [DDPS-4770]
- Server Configuration Tool error handling is improved. [DDPS-4786]
- Importing the same certificate for Server Encryption (SSOS) that is imported as the SSL certificate is now blocked, with an error message that the certificate cannot be imported twice. [DDPS-4805]
- The Pending Value field now displays the correct value in the Compliance Reporter Pending Policy Detail Report. [DDPS-4840]
- SED data time stamps are now preserved when recovery data is archived. [DDPS-4877]
- A Cloud Profile Update poll no longer results in uncommitted policies. [DDPS-4878]
- An issue is resolved that resulted in an Internal Error when **Reporting** > **Audit Events** is selected in the Remote Management Console. [DDPS-4882]
- The Policy Proxy Polling Interval value is now correct in the Compliance Reporter Effective Policy Report. [DDPS-4927]
- Importing a valid certificate with Server Configuration Tool now succeeds after importing an invalid certificate. [DDPS-4928]

Technical Advisories v9.7

- Setting an Action in a Client Firewall rule to Block IPv4 traffic prevents client connectivity with the Dell Server. Do not set such an Action when running in Connected Mode. [DDPC-5716]
- The Client Firewall and Web Protection features of Endpoint Security Suite Enterprise v1.4 require Enterprise Server v9.7 or later. Before upgrading clients to use these features, Enterprise Server v9.7 or later must be installed and the policy, Memory Action: Exclude executable files, must be ***enforced*** on pre-v1.4 clients. Prior to client upgrade to the new features, refer to Default Policy Changes for the policy's new default value. Do not begin client upgrade before the new policy is enforced on the client. [DDPS-5112]
- Amended 7/2017 - SMTP settings are not retained during a Recovery Installation and must be reconfigured using the Server Configuration Tool after recovery is complete. [DDPS-5239]
- Added 7/2017 - Enterprise Server does not support .local domains. [DDPS-5334]

New Features and Functionality v9.6

- Dell Enterprise Server is now supported with the following:
  - Windows Server 2016
  - SQL Server 2016
- Dell Enterprise Server now supports Advanced Threat Prevention and Encryption on persistent and non-persistent VMware and Citrix VDI clients.
- Secure Lifecycle audit events logs can now be exported to SIEM.
- New Server Encryption policies allow the administrator to configure the maximum number of attempts and retry interval for connection to the Dell Server.
- Remote PBA management of local user accounts is now available.
- New policies and functionality support the Disconnected Mode beta release.

Resolved Technical Advisories v9.6

- The tool tip for the Audit Control policy, Client Retention Storage, now indicates that maximum storage is measured in megabytes. [DDPS-3682]
- An issue is resolved that resulted in an occasional database migration error during a new installation. [DDPS-3792]
- The installer error message that occurs when a hostname includes an underscore, which is not allowed, is now more specific. [DDPS-3902]

- A data access error no longer occurs in the Remote Management Console when the default language of a SQL profile is not English. [DDPS-4349]
- A non-domain endpoint is no longer reported as unprotected in the Remote Management Console if the user has logged in more recently than other users on an endpoint and that user has a pending or incomplete encryption sweep. [DDPS-4470]
- The Secure Lifecycle agent is now correctly named on the Remote Management Console Endpoint Details & Actions tab. [DDPS-4512]
- An external Secure Lifecycle user can no longer access protected documents after their domain is removed from the Full Access list (previously, whitelist), regardless whether the user is individually granted Full Access/whitelisted. [DDPS-4602]
- Added 08/2018-Registration is now successful when an external user registers to use Data Guardian with a Front End server installed. [DDPS-4603]
- Password complexity rules are now enforced when a Secure Lifecycle external user resets the password. [DDPS-4604]
- Filtering with the Removed field in the Compliance Reporter BitLocker Manager Detail-TMP Aware report now returns correct results. [DDPS-4608]
- Forensic key retrieval now proceeds as expected when one or more key_id instances is invalid. [DDPS-4689]

Resolved Customer Issues

- Enabling non-domain activations in the server_config.xml file now succeeds as expected, without regard to case sensitivity of the value entered for the property, accountType.nonActiveDirectory.enabled. Also, Compatibility Server logs now indicate when enabling non-domain activation fails due to case-sensitivity issues with the property name, itself. [DDPS-4068]
- An issue is resolved that resulted in a Security Server Java instance failure with the following error message: EXCEPTION_ACCESS_VIOLATION. [DDPS-4245]
- An issue is resolved that resulted in uncommitted policies that were not initiated by the administrator. [DDPS-4761]
- Added 05/2018- Dell Security Management Server selects policies based on the group in which endpoints are in no longer instead of arbitrated policies. The group with the highest precedence value succeeds, and no other groups are considered. [DDPS-5377]

Technical Advisories v9.6

- If the ProgramData folder is open during an upgrade, an error displays: "C:\ProgramData\Del\GateKeeper is unavailable...." To work around this issue, close the ProgramData folder and click **OK** in the error dialog. [DDPS-4573]
- When running Compliance Reporter with Google Chrome, the date selection calendar does not display in the Value column when the **Created** * field is selected in Filter Fields area of the Report Layout. [DDPS-4691]
- Added 4/2017 - Threat Protection Status categories differ between Remote Management Console Dashboard Notifications and Email Notification Summaries. Dashboard Notification categories are Critical, Major, Minor, and Warning. Corresponding email notification categories are Critical, High, Medium, and Low. [DDPS-4802]

New Features and Functionality v9.5

- Added 8/28 - A new policy is added that enables administrators to force Policy-Based Encryption when a SED is detected.
- Dell Enterprise Server now supports Secure Lifecycle. Secure Lifecycle provides data security, wherever it goes - data at rest, data in motion and data in use - through encryption. Data Loss Prevention (DLP) ensures no data is lost in motion or in flight, while Data Rights Management (DRM) defines access and usage control. Additionally, file monitoring provides detailed data usage visibility to support forensics needs. Secure Lifecycle provides security, authority, visibility, and cross-platform compatibility - all through a single solution - with the following features:
  - Auditing and reporting on file activity, files synced, files accessed by whom, where and when, and compliance reporting.
  - Geolocation with map visualization as well as multiple filtering options for audit events.
  - Enforcement of whitelists/graylists/blacklists of email domains and addresses for control over file sharing.
  - Enforcement of policies for access to cloud services, folders, and applications.
  - Management of key expirations and polling periods.
  - Ability of administrators to monitor all known IP addresses for cloud service providers and match them with the application process to centrally manage encryption, encryption keys, data recovery, policies and forensics.

  Secure Lifecycle Protected Office mode offers enhanced security on Office documents (Word, PowerPoint, and Excel) for internal users.
  - Files remain encrypted for unauthorized users, for example, when files are attached in email, moved in a web browser or File Explorer, or stored on removable media.
  - A callback beacon can be inserted into every protected Office file, when the beacon server is installed as part of the Front End server installation.
- As of v9.4.1.6,Dell Enterprise Server supports Advanced Threat Prevention on Mac computers. Advanced Threat Prevention provides real-time threat detection by analyzing potential file executions for malware in both the operating system and memory layers to

prevent the delivery of malicious payloads. Control of execution at the endpoint allows for accurate and effective detection of malicious threats - even those that have never been seen before. Advanced Threat Prevention uses machine learning techniques that allow detection of new malware, viruses, bots and unknown future variants, where signatures and sandboxes fail. Memory protection strengthens basic operating system protection features by providing an additional layer to detect and deny certain behaviors that are commonly used by exploits.

- As of v9.5, Cloud Edition is no longer supported.

Resolved Technical Advisories v9.5

- When an existing certificate is imported during upgrade, the installer no longer displays an error if the certificate password has been changed from the default password. [DDPS-2644]
- Searching for endpoints in the Remote Management Console using the Shield Recovery ID now returns expected results. [DDPS-4017]
- An issue is resolved that resulted in Summary Statistics in the Remote Management Console Dashboard occasionally not updating as expected. [DDPS-4082]
- A second or subsequent notification that is added in Notification Management in the Remote Management Console no longer retains the Type and Priority values of the previously added notification. [DDPS-4178]
- After upgrade, the Compliance Reporter reports, SED Authentication Method Policy Detail and Windows Encryption Failures and Sweep Status, are available as expected. [DDPS-4183]
- After the user browses for the Service Account Run As user name, the credentials now populate in the Service Runtime Account Information dialog in the installer. [DDPS-4234]
- The Advanced Threat Prevention category is now populated in Log Analyzer in the Remote Management Console. [DDPS-4241]
- An issue that resulted in failure of Advanced Threat Prevention Agent Auto Update enrollment is resolved. [DDPS-4244]
- The Add User and Add Group options are removed from Domain Detail for Members of Non-Domain Users in the Remote Management Console. These options are not applicable for non-domain users. [DDPS-4255]

Resolved Customer Issues

- The Specification field in the Remote Management Console Add Endpoint Group page is now validated for length and displays an error if more than 4,000 characters are entered. [DDPS-2953, DDPS-4260]
- The TPM Enabled field in the Compliance Reporter BitLocker Manager Detail report is now accurate. [DDPS-3394]
- During new database installation, the installer now creates the database in the folder configured in Server Properties Database Settings rather than in the master database folder specified in Database Properties Files. [DDPS-4221]

Technical Advisories v9.5

- Amended 7/2017 - The Remote Management Console **Login** button may be disabled in Google Chrome or Internet Explorer on Server 2012. To work around this issue, clear the browser cache and then attempt login or use Mozilla Firefox 41.x or later. [DDPS-4558]
- Advanced Threat Prevention policies are not properly validated if their values are not enclosed in double quotes (") and contain wildcards or special characters, including commas (,), brackets ([ ]), and tildes (~). To force validation, enclose strings in double quotes ("). Do not use wildcards and special characters, which are not allowed. [DDPS-4589]
- Added 2/2017 - Policy validation beginning in v9.5 may result in an "Error Validating Policy " message in the Remote Management Console when attempting to view policy when the value of the policy is incorrectly formatted. To work around this issue, correct the formatting of affected policy values. To identify the affected policies, follow these steps:

  1. Open <Core Server install directory> **PolicyService.config**.

     Enterprise Server - Program Files\Dell\Enterprise Edition\Core Server

     VE - /opt/dell/server/core-server
  2. Change the StrictValidation property value from **true** to **false**: `<property name="StrictValidation" value="false"/>`
  3. Restart the services.
  4. In the Remote Management Console, navigate to view policy at the level where the Error Validating Policy previously occurred, and note the policy name identified in the error.
  5. Correct the policy value formatting, and click **Save**.
  6. In the left pane, click **Management** > **Commit**, enter the policy change description, and click **Commit Policies**.
  7. If desired, change the StrictValidation property value from **false** back to **true**, to re-enable policy validation.

  [DDPS-4779]

New Features and Functionality v9.4.1.6

- Dell Enterprise Server now supports Advanced Threat Prevention on Mac computers. Advanced Threat Prevention provides real-time threat detection by analyzing potential file executions for malware in both the operating system and memory layers to prevent the delivery of malicious payloads. Control of execution at the endpoint allows for accurate and effective detection of malicious threats - even those that have never been seen before. Advanced Threat Prevention uses machine learning techniques that allow detection of new malware, viruses, bots and unknown future variants, where signatures and sandboxes fail. Memory protection strengthens basic operating system protection features by providing an additional layer to detect and deny certain behaviors that are commonly used by exploits.

New Features and Functionality v9.4.1

- A new Advanced Threat Prevention Agent Auto Update feature is available and can be enabled from Services Management in the left pane of the Remote Management Console. Enabling Agent Auto Update allows clients to automatically download and apply updates from the Advanced Threat Prevention server. Updates are released monthly.
- New Advanced Threat Prevention policies allow the administrator to configure automatic handling upon detection of a malicious payload and extended Script Control settings for Active Scripts, PowerShell, and Office macros.
- The Advanced Threat Events Report can now be exported as an Excel or .csv file from the Advanced Threat Events tab in the Remote Management Console.
- A new policy allows the administrator to hide encryption icons in File Explorer for managed users.

Resolved Technical Advisories v9.4.1

- Dell will continue to support current versions of Dell Enterprise Server on third-party software platforms as long as it is technically and commercially reasonable for Dell to do so, when there is no external dependency. Due to external dependency, VMware ESXi 5.1 is no longer supported as of the v9.4.1 release. For more information, see http://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/support/product-lifecycle-matrix.pdf.
- An error no longer occurs during forensic key bundle download from Dell Enterprise Server. [DDPS-3244]
- The Inventory Received field on the Endpoint Detail page of the Remote Management Console is now populated upon activation of an endpoint. [DDPS-3982]
- Notification emails are now sent as expected when All Notification Types are selected when configuring Notification Management in the Remote Management Console. [DDPS-4003, DDPS-4038]
- An issue that resulted in an internal error when clicking Device Recovery Keys on an Endpoint Detail page in the Remote Management Console is resolved. [DDPS-4222]

New Features and Functionality v9.4

- The Remote Management Console now features enhanced configurable Dashboard and Email Notifications, to update administrators about threat events, certificate expirations, license availability, configuration changes, product updates, and knowledge base articles.
- Advanced Threat Prevention customers can now take advantage of these capabilities, available in the Remote Management Console:
- Certificates can now be imported and added to the Safe list.
- Security Information Event Management (SIEM) software can be integrated to capture Advanced Threat events.
- Enhanced data about threats and devices on which they are identified is now available.
- The File Folder Encryption policy category in the Remote Management Console has been renamed to Policy-Based Encryption.
- The Alerts Management menu item in the Remote Management Console has been renamed to Notification Management.
- Dell Enterprise Server installations are no longer supported on 32-bit operating systems.

Resolved Technical Advisories v9.4

- The installer no longer accepts underscores in host names. An underscore character ("_") in either the Compatibility Server host name or Security Server host name causes connection to that Server to fail. A host name cannot contain an underscore character ("_"), due to a Java platform issue, JDK-6587184. For more information, see http://bugs.java.com/view_bug.do?bug_id=6587184. [DDPMTR-1345, DDPS-3570]
- The policy values in the BitLocker Manager Policy report are now correctly populated, and managed devices no longer display on duplicate rows. [DDPS-2810, DDPS-3427]
- Dell Enterprise Server now supports multiple entitlements associated with a single service tag. [DDPS-2949]

- Added 7/2017 - The Administrator Roles topic in AdminHelp no longer indicates that the System Administrator can commit policies, recover data, and recover endpoints, and the Security Administrator can delegate administrator rights, although these administrators do not have these permissions, and now correctly indicates that Account administrators can delegate administrator rights. [DDPS-3004, DDPS-3005, DDPS-3006]
- The valid key format is now downloaded from Enterprise Server in Enterprise Edition for Mac recovery files, and an issue that resulted in the Server delivering blank FileVault recovery keys is resolved. [DDPS-3139, DDPS-3873]
- Domains with names that include spaces or special characters can now be added in the Remote Management Console. [DDPS-3329]
- Domain Alias Names are now resolved as expected in the Remote Management Console, and login with an invalid Domain Alias no longer succeeds. [DDPS-3330, DDPSUS-767]
- The Compliance Reporter Advanced Threat Prevention Events report now includes the Type field, which displays the threat type. [DDPS-3331]
- Dropbox for Business remote wipe function is available in the Remote Management Console. [DDPS-3333]
- Administrators can now update Domain Settings in the Remote Management Console after their user credentials are changed in Active Directory and when the Active Directory server or service is unavailable. A "Failed to Retrieve Domain" or "'code':10180" message no longer displays. [DDPS-3336, DDPS-3337, DDPS-3338]
- Entering any combination of upper- and lower-case characters in Compliance Reporter settings now returns expected results. [DDPS-3369]
- An issue that led to Remote Management Console timeouts when searching for endpoints is resolved. [DDPS-3400]
- An issue that caused an error during installation on servers with heavily loaded processors is resolved. [DDPS-3444]
- Administrators with UPNs exceeding 32 characters can now effectively send SED commands to devices. [DDPS-3432]
- An issue that led to an internal error in the Remote Management Console is resolved. [DDPS-3454]
- Provisioning the Advanced Threat Prevention service now proceeds as expected when used with a proxy server. [DDPS-3475]
- The backup folder is now preserved following an installation rollback during upgrade. [DDPS-3527]
- Policy template settings that include the Rijndael value now migrate properly during upgrade. [DDPS-3531]
- Logging is improved for the error that results when a user with duplicate UPNs in the Dell Data Protection database attempts to log in to the Remote Management Console. [DDPS-3578]
- Logging is improved for the error that results when searching for a user whose group name includes a special character. [DDPS-3587]
- The Common Encrypted Folders policy is now correctly applied to %ENV:USERPROFILE%\Downloads. [DDPS-3752]
- Endpoints that were previously removed can now be consistently added back into inventory and receive new policies as expected. [DDPS-3772]
- The Remote Management Console Domain Details & Actions page is no longer illegible if the domain service account that is used to add the domain includes a quotation mark (") in its password. [DDPS-3813]
- The Save option is now available when the SQL Authentication password is updated in the Server Configuration Tool. [DDPS-3817]
- An issue that led to high Compatibility Server CPU load at restart when forensics are enabled in the Security Server is resolved. [DDPS-3833]
- An error that caused occasional Core Server service crashes when multiple inventories are run is now properly handled. [DDPS-3877]
- An internal error no longer displays on the Effective Policies page for an Endpoint or User after upgrade from a pre-v9.2 Enterprise Server. [DDPS-4000]

Technical Advisories v9.4

- After Dell Enterprise Server and DDP Enterprise Server - Virtual Edition installation, the Remote Management Console displays "1 Uncommitted Override," indicating a pending policy commit. The policy represents an internal setting. To work around this issue, commit policies after installation. In the left pane, click **Management** > **Commit**, enter the description, "Initial commit," and click **Commit Policies**. [DDPS-3163]
- If either the SQL database or SQL instance is configured with a non-default collation, installation fails. A non-default collation must be case-insensitive. For a list of collations and case sensitivity, see https://msdn.microsoft.com/en-us/library/ms144250(v=sql.105).aspx. [DDPS-3355]
- In order for Dell Data Protection SED and HCA v8.5.1 and earlier clients to communicate with Dell Enterprise Server and Virtual Edition v9.4, the following settings must be configured on the Server:

1. On the Security Server, access <installation folder>\Enterprise Edition\Security Server\conf\spring-jetty.xml, and comment out the excludeProtocols property:

   <!--

   <property name="excludeProtocols" value="SSL,SSLv2,SSLv3" />

   -->
2. In the ..\Dell\Java Runtime\jre1.8\lib\security\java.security file, remove "SSLv3, " from the line below:

   jdk.tls.disabledAlgorithms=SSLv3, RC4, DH keySize < 768

[DDPS-3371]

- Universal security groups are not supported due to the way they are created within Active Directory. [DDPS-3765]

New Features and Functionality v9.2

- Dell Enterprise Server now supports Advanced Threat Prevention. Advanced Threat Prevention provides real-time threat detection by analyzing potential file executions for malware in both the operating system and memory layers to prevent the delivery of malicious payloads. Control of execution at the endpoint allows for accurate and effective detection of malicious threats - even those that have never been seen before. Advanced Threat Prevention uses machine learning techniques that allow detection of new malware, viruses, bots and unknown future variants, where signatures and sandboxes fail. Memory protection strengthens basic operating system protection features by providing an additional layer to detect and deny certain behaviors that are commonly used by exploits.
- The Remote Management Console has a new look and feel, with a responsive HTML 5 design that can be viewed on virtually any screen size. It no longer requires installation and is now accessed at this URL:

  https://server.domain.com:8443/webui/
- The Remote Management Console now offers the following new features and capabilities:
  - Email alert notifications can be set for Threat Protection and Advanced Threat Prevention events.
  - When data is recovered on a computer with more than one self-encrypting drive, each drive can be individually selected for recovery.
- Amended 07/2016 - The Console Web Service component is no longer used as of v9.2, with the removal of the Silverlight Console.

Resolved Technical Advisories v9.2

- Further research into entitlement issues yielded testing improvements, resulting in the resolution of some open and unresolved issues. [DDPMTR-1768, DDPS-1571, DDPS-1716/DDPSUS-235]
- A few items on Remote Management Console screens that were previously untranslated are now translated. [DDPS-846, DDPS-1519, DDPS-1525, DDPS-1722, DDPS-1928]
- The Compliance Reporter Effective Policy Report now displays Gatekeeper connections and the correct value type for the Policy Proxy Polling Interval policy. [DDPS-1233]
- When a non-domain computer is joined to the domain, duplicate endpoint entries no longer display in the Remote Management Console, and the endpoint properly receives policies. [DDPS-1304]
- The Compliance Reporter Administrator List Report now includes the Group Name field. [DDPS-1720]
- In the Remote Management Console, when Client Firewall rules are added or edited, the executable Signed by field is now validated. [DDPS-1794/DDPSTE-445]
- When retrieving the BitLocker Manager recovery password in the Remote Management Console for more than one volume, the first recovery password is now cleared before second and subsequent BitLocker volumes are selected. [DDPS-1808]
- Uninstallation with setup.exe no longer requires reboot. [DDPS-1839]
- At the end of Server installation, the check box next to Show windows installer log is now visible. [DDPS-1840]
- Permissions that are inherited from a group are now removed from Remote Management Console administrators when the group is removed. [DDPS-1853]
- The Compliance Reporter Local Policy Report now includes device-based policy changes made at the Endpoint Group and Endpoint levels. [DDPS-1859]
- The error message that displays when the Core Server is running during Server Configuration Tool startup no longer states that the Compatibility Server must be stopped. The Server Configuration Tool functions properly when the Compatibility Server is running. [DDPS-1863]
- The new name of a renamed computer now replaces the previous name rather than displaying as a second endpoint in the Remote Management Console when keys are escrowed before the new computer name is processed in inventory. [DDPS-1895]
- The Cloud Storage policy, OneDrive Message, is no longer applicable and is now removed from the Remote Management Console. [DDPS-1917]
- An upgrade now proceeds as expected after a previous upgrade is canceled. [DDPS-2065]
- The default Cloud Encryption Help File delivered to endpoints through the Help File Contents policy now renders properly on endpoints. [DDPS-2071]
- The Mac recovery bundle now includes the hostname and extension in the Save dialog that displays on the endpoint. [DDPS-2090]
- An Unknown Exception no longer occurs during upgrade after users have been manually removed from Active Directory. [DDPS-2330]
- Inventory polls for managed clients have been reduced from twelve to two hours to more accurately reflect status changes. [DDPS-2371]
- An issue that caused some failures of services startups, on-the-box entitlement retrievals, and Compliance Reporter startups after installation or upgrade when configuration changes are made through the Server Configuration Tool has been resolved. [DDPS-2755]

- When an endpoint is moved from one Endpoint Group to another non-default Endpoint Group, Endpoint Group policies are now consistently applied based on Precedence settings. [DDPS-2881]
- A default SDE Encryption Rules policy which caused problems with Windows updates has been resolved. The issue resulted from encryption of \System32 executable files. The default policy has been changed for EE and VE Servers v9.2 and later. [DDPS-2952, DDPC-1207]

Technical Advisories v9.2

- A Compliance Reporter report layout can be deleted without an error message although subordinate reports are attached to it. [DDPS-1094]
- The IP Exclusions for Web Protection field in the Remote Management Console accepts invalid formats. [DDPS-2206]
- The description of a custom Client Firewall rule in the Remote Management Console does not include local or remote network type. [DDPS-2278]
- If browser cookies are not enabled, the message "An internal error occurred" displays at logon to the Remote Management Console rather than a message prompting the user to enable cookies. [DDPS-2661]
- The Compliance Reporter Mobile Device Policy report is not populated. [DDPS-2675]
- In Compliance Reporter Report View Scheduling, the tooltip for the Email Recipients field says that email addresses can be separated by commas or placed on separate lines. Email addresses cannot be placed on separate lines but should be separated by commas. [DDPS-2678]
- During services restart, navigating to the Enterprise Population pages in the Remote Management Console results in an Access Denied message rather than a return to the login page. [DDPS-2815]
- After the Advanced Threat Prevention service is provisioned, Advanced Threat Events do not begin to display until the administrator logs off then logs back on to the Remote Management Console. [DDPS-2816]
- The Remote Management Console Endpoint Security Policies tab shows values for the BitLocker Recovery Information to Store in AD DS policy as *Recovery Passwords and Keys Packages* and *Recovery Passwords Only*. In Endpoint Effective Policies, the values for the same policy are *Passwords and Keys* and *Passwords Only*. [DDPS-2821]
- The Client Firewall custom rule allows the administrator to enter subnet addresses although subnets cannot be created for local or remote networks. [DDPS-2838]
- A few tooltips and areas of a few pages are not localized in the Remote Management Console. [DDPS-2842, DDPS-2844, DDPS-2989, DDPS-2994, DDPS-2996, DDPS-2997, DDPS-2999]
- "Override Count" is truncated on the Endpoint Security Policies tab in the Spanish, Italian, French, Portuguese, and Brazilian Portuguese Remote Management Console. [DDPS-2843]
- The AdminHelp icon is not available from the Remote Management Console login screen. [DDPS-2858]
- The Remote Management Console User Detail tab displays the Effective Policies icon for mobile devices although effective policies do not apply to mobile devices. [DDPS-2880]
- There is a delay between completion of the Server poll based on the configured Server Polling Interval and display of Threat Protection events in the Remote Management Console. [DDPS-2896]
- The refresh button is not functioning on the Alerts Management page in the Remote Management Console. [DDPS-2923]
- The Add Domain page in the Remote Management Console has no vertical scrollbar, so on small screens or screens with low resolution, the Add Domain button is not visible. [DDPS-2945]
- Entering an invalid LDAP password when adding a domain in the Remote Management Console results in a prompt to check the logs rather than a message that the password is invalid. [DDPS-2954]
- The Remote Management Console does not function if TLS v1.0 is disabled. [DDPS-2955]
- When adding a User in the Remote Management Console, searches for users who belong to a large number of Active Directory groups may take longer than expected. If this occurs, clicking the Search button more than once on the Add Users by Domain dialog can cause the Security Server to crash. Do not click the Search button more than once on the Add Users by Domain dialog. [DDPS-3010]
- If an invalid hostname is entered during Advanced Threat Prevention Service setup, a timeout occurs. To work around this issue, click OK in the Timeout dialog to return to the Services Management page. Verify the hostname, and begin Advanced Threat Prevention Service setup again. [DDPS-3019]
- Email alerts of Advanced Threat Prevention events are not being sent. [DDPS-3031]

New Features and Functionality v9.1.5

- Cloud storage provider profiles are now automatically updated daily on Dell Enterprise Server. Updates are delivered to Dell Data Protection | Cloud Edition clients when policies are committed.

Resolved Technical Advisories v9.1.5

- In Compliance Reporter, the Mobile Policy report now includes results for all activated mobile devices. [DDPMTR-838]
- During an upgrade when the SQL database is unavailable, the upgrade now continues without delay. The Server Configuration Tool can be used to migrate the database when it is available. [DDPMTR-1226]
- When the option Re-use SSL certificate for SSOS is selected during a new installation, the SSL certificate is reused as expected. [DDPMTR-1243]
- The Compliance Reporter Email Recipients field now accepts only a comma (",") as a separator rather than accepting special characters. [DDPMTR-1257]
- The setting field of the Threat Protection policy, Exclude Processes, no longer accepts invalid values in the Remote Management Console. [DDPMTR-1346]
- Dell Enterprise Server v9.1.5 includes a security update addressing an OpenSSL vulnerability (OpenSSL CVE-2015-4000). Customers and field teams should take v9.1.5 and all Dell Enterprise Server updates or sustaining releases as a best practice. [DDPMTR-1507]
- Performance is improved for client activations based on streamlined access of Active Directory. [DDPMTR-1538]
- Import of certificates with spaces in alias names is improved. [DDPMTR-1611]

Technical Advisories v9.1.5

- Migration to a version later than v9.0 fails when using a Microsoft SQL 2005 database. [DDPMTR-1633]
- Added 02/2016 - After migration to v9.1.5, the Domain Users group in the Remote Management Console does not display all users in the group. [DDPS-1937]
- Added 02/2016 - The Remote Management Console displays unprotected status for EMS-encrypted USB drives. [DDPS-2835]

New Features and Functionality v9.1

- Forensic Administrator rights for a User Group can now be delegated by the Superadmin or Security Administrator to a member of the User Group.
- Server Encryption is now supported, featuring port control and removable storage encryption as well as support for maintenance scheduling, which allows control over enforcement of policies that require reboot.
- Deferred Client Activation is now supported, allowing an enterprise to extend centrally managed encryption policies to users' devices in a BYOD environment.
- New policies allow administrators to suppress or filter Endpoint Security Suite popup notifications on client computers. This update is supported with Endpoint Security Suite v1.1.1 and later clients.
- Support for user feedback to Dell is now available through policy for most Dell Data Protection clients.

Resolved Technical Advisories v9.1

- When Client Firewall rules are added or edited in the Remote Management Console, Custom EtherType now accepts only four characters, and values entered into the Domain name field are now validated. [DDPMTR-528, DDPMTR-732]
- In the Remote Management Console, when Core Networking rules are added or edited, the Connection types field is now locked as expected and cannot be edited. [DDPMTR-562]
- In the Remote Management Console, an endpoint that has been previously removed can now be recovered. [DDPMTR-640]
- In the Remote Management Console, in Default/Custom Firewall rules, an "Invalid Signer" error no longer displays when an executable is edited. The additional error present only in the Silverlight Console, "Specify one or more of the following required...," also no longer displays. [DDPMTR-730, DDPMTR-1156]
- Authorization of the link between the Server and Dropbox now succeeds when Cloud Edition is deployed. [DDPMTR-748]
- When Cloud Edition is deployed and an external user activates against the Server, on the User Details page in the Remote Management Console, the User Type no longer incorrectly displays as "AD." [DDPMTR-762]
- In the Remote Management Console, when an attempt is made to import an invalid or duplicate license, the previous generic error message has been replaced with a message that more clearly describes the error. [DDPMTR-764]
- The Secure Windows Credentials policy is now correctly grouped with Fixed Storage Policies rather than with General Settings policies. The SDE Encryption Enabled policy must be set to True in order for the Secure Windows Credentials to be applied. [DDPMTR-786, DDPSTE-638]
- In the Compliance Reporter Mobile Device report, time stamps for commands sent to mobile devices are now correct. [DDPMTR-839]
- In the Remote Management Console, Log Analyzer - Admin Actions now displays accurate data for endpoint policy changes, and System Logs now displays login entries for users from sub-domains. [DDPMTR-911, DDPMTR-991]
- After uninstallation, wrapper logs are now removed as expected. [DDPMTR-913]

- The Threat Protection Security policy now disables all Threat Protection policies and features. [DDPMTR-1011]
- The Host Name field is now selected for inclusion by default and Host Names displayed in the Report Result are now correct in the Compliance Reporter Threat Protection Details report. [DDPMTR-1014]
- Active Directory reconciliation no longer fails when one of multiple domains is offline or inaccessible on the network. [DDPMTR-1153]
- Amended 02/2016 - In the Silverlight Console, an issue with the way cookies are handled that resulted in login failure with the error, "Unable to Access User Admin Roles," has been resolved. [DDPMTR-1176]
- The upgrade error that occurred with an error logged regarding the UserEntity table, EID column is now resolved. [DDPMTR-1237]
- The Threat Protection Security policy now disables all Threat Protection policies and features. The three policies, Malware Protection, Client Firewall, and Web Protection, no longer have to be individually set to False. [DDPSTE-451, DDPMTR-1011]

Technical Advisories v9.1

- In the Remote Management Console, fields for policies with numeric values accept a "+" or "-" character immediately preceding the policy value. To work around this issue, ensure that these characters are not included in policies' values before the policies are committed. [DDPMTR-765]
- When running DDP|E with Deferred Activation, Cloud Edition policies may not flow from the DDP Server. If this occurs, in DDP Remote Management Console, check the list of endpoints. The list includes both the host name and the Machine ID for the computer. To work around this issue, ensure that Cloud Edition policies are set for the endpoint represented by the computer host name. DDP|E policies must continue to be set on the endpoint represented by the computer Machine ID. [DDPMTR-825]
- If Compliance Reporter default reports have been customized prior to upgrade, the previous version of customized reports must be restored in order to continue to use them. However, after the previous version is restored, new reports included in the upgrade are not available. [DDPMTR-870]
- When a self-signed certificate is created at installation, the certificate is valid from a time approximately six hours later than the installation time, rather than being immediately valid. To work around this issue, on the Settings tab of the Server Configuration Tool, check Disable Trust Chain Check. [DDPMTR-1195]
- Added 09/2015 - The CIDR format must be used to specify a subnet in Firewall Settings in the Remote Management Console. [DDPMTR-1253]
- In the Remote Management Console, when Client Firewall rules are added or edited and ICMP Transport Protocol is selected from the Transport drop-down menu, the Message Type displays the default message type as "Echo-Replay" instead of "All," as expected. [DDPMTR-1254]
- When using Windows Authentication to perform a new installation or upgrade, if the credentials of the logged on user differ from the credentials of the domain services account and a certificate from a signing authority is used, the certificate must be stored in a folder that is accessible during installation to both the domain services account and the logged on user. If the credentials of the logged on user differ from the credentials of the domain services account and a self-signed certificate is used, before beginning installation or upgrade, you must log in with the domain services account credentials. [DDPSUS-406]

New Features and Functionality v9.0

- Dell Enterprise Server now supports Endpoint Security Suite with an extensive set of new policies and Compliance Reporter reporting options. Endpoint Security Suite includes the following:
- Malware Protection
- Client Firewall
- Web Protection
- DDP|E Encryption
- SED Management
- Advanced Authentication
- BitLocker Manager

Resolved Technical Advisories v9.0

- AdminHelp now correctly states that the value OneTimePassword rather than One-time Password can be set for the logon and in-session policies. [DDPS-1594]
- In localized versions of the Remote Management Console installer, the Host dialog banner is now properly sized. [DDPSTE-275]
- When Enterprise Server is uninstalled, the LSARecovery.log file is now removed, as expected. [DDPSTE-308]
- AdminHelp now correctly states the default Server Polling Interval for TPM and SED System Settings as 720 minutes, and the Cloud Storage Server Polling Interval range is now specified as 1-1440 minutes. [DDPSTE-486, DDPSTE-586, DDPSTE-591]
- In the Silverlight Console, an Unhandled Error that previously occurred when accessing a specific user's User Groups tab is now resolved. [DDPSTE-487]

- Logging on to the Silverlight Console from Windows 8.1 no longer results in an unhandled exception. [DDPSTE-499]
- A few previously unlocalized areas of Remote Management Console screens are now localized. [DDPSTE-501, DDPSTE-502, DDPSTE-503]

Technical Advisories v9.0

- In the Silverlight Console, title bars for Firewall Edit Rule dialogs are incorrectly titled. [DDPMTR-672]
- In Compliance Reporter EMS Event and Mobile Device Detail Report Result pages, some columns and the bottom scroll bars are not visible. [DDPMTR-969]
- In the Remote Management Console, when duplicate entries of a Mobile Edition endpoint exist, selecting the Resolve User option returns an error and does not resolve the duplicate entries. [DDPSTE-371]
- In the Remote Management Console, when Client Firewall rules are added or edited, the IP address and Network type fields are not validated; column headers can be moved and resized to the extent that headings become illegible; multiple rows can be selected, preventing them from being edited; the Cancel button is unresponsive in the Add and Edit dialogs; and an executable that is added does not display until the rule is closed then reopened. [DDPSTE-414, DDPSTE-415, DDPSTE-421, DDPSTE-426, DDPSTE-430, DDPSTE-431, DDPSTE-437, DDPSTE-443]
- In the Remote Management Console, when Client Firewall rules are added, the Add dialog occasionally freezes when incorrectly formatted values are entered. To work around this issue, click the close button in the upper right corner of the dialog then click the Add button under Specify Networks to reopen the dialog. [DDPSTE-432]
- When performing a Remote Wipe on an iOS device that is managed through EAS, although the Remote Wipe is successful and an Acknowledged time and date stamp display in Enterprise Server, an error is logged in Policy Proxy and EAS server logs. [DDPSTE-529]
- A Mobile Edition license is not consumed when a mobile client is activated. [DDPSTE-549]
- The Key Server log file, log.txt, is stored in `C:\<installpath>\Dell\Enterprise Edition\Key Server` rather than in C:\<installpath>\Dell\Enterprise Edition\Key Server\logs, as expected. [DDPSTE-637]
- If a custom value is used for the Message Broker TCP Port, after a new installation or upgrade from a pre-v8.5 Enterprise Server, the value must be manually configured. For a new installation, open <Compatibility Server install dir>\conf\server_config.xml and change the broker.port value to the correct port number. For an in-place upgrade from a pre-v8.5 Enterprise Server, change both the broker.port value in the server_config.xml file and the activemq.port.tcp value in Message Broker\conf\application.properties to the correct port number. [DDPSTE-654]

Resolved Technical Advisories v8.5.1

- Silverlight Console connectivity is improved when Enterprise Server is constrained. [DDPS-239]
- Enterprise Server v8.5.1 includes a security update addressing an OpenSSL vulnerability (OpenSSL CVE-2014-3566). Customers and field teams should take v8.5.1 and all Enterprise Server updates or sustaining releases, as a best practice. [DDPS-1541]
- In multi-level domain environments, users can now successfully log on to the Remote Management Console. [DDPS-1559, DDPSTE-274]
- Search results are now as expected when searching for Endpoints that include a wildcard (*) in the Hostname. [DDPS-1575, DDPSTE-402]
- Licensing issues have been resolved. [DDPS-1584, DDPSTE-403, DDPSUS-58]
- Added 02/2016 - Client activations are now successful after migration from v6.8. [DDPS-1657]
- Pre-v8.5 DDP|E SED and HCA clients that have a PBA activated now receive policy updates as expected when settings for Logon Authentication and In-Session Authentication policies include One-time Password as a value. [DDPSTE-439]
- The in-use license count for Mobile Edition is now properly calculated. [DDPSUS-61]
- TLS communication security is hardened. [DDPSUS-108]
- On Brazilian Portuguese operating systems, the Silverlight Console's webhelp now functions properly.

Technical Advisories v8.5.1

- Amended 04/2015 - To protect communications against the OpenSSL CVE-2014-3566 vulnerability, Dell Enterprise Server v8.5.1 and later are set to communicate using TLS, by default. However, DDP|E SED and HCA v8.5 and earlier clients communicate with Enterprise Server using SSL. This means that when running Enterprise Server v8.5.1 and later, DDP|E SED or HCA v8.5 and earlier clients with Preboot Authentication activated will fail to communicate with Enterprise Server. To work around this issue, search "SLN296006" at www.dell.com/support, to find the knowledge base article associated with this issue. This workaround must be implemented as soon as possible, in order to prevent PBA client communication issues with Enterprise Server v8.5.1 and later. [DDPS-1609]

New Features and Functionality v8.5

- Dell Enterprise Server now supports automated migration from DDP Personal Edition to Enterprise Edition with the DDP Managed Migration Utility.
- Dell Enterprise Server now supports new Cloud Edition policies that offer expanded protection and management options. When Cloud Edition is used with Dropbox for Business, the following features are now available:
  - The Dropbox for Business administrator can now remote wipe a Dropbox for Business account.
  - New policies offer multi-account support, providing the capability to distinguish between Dropbox for Business and Dropbox personal accounts.
- Dell Compliance Reporter offers new reporting options:
  - A new Cloud Users report displays enrollment and remote wipe information about Dropbox for Business users.
  - New filtering options are available with the Cloud Edition Encrypted Files/Actions report to provide greater customization of event and key management detail.
  - The Device Detail report now includes a field to indicate devices that have self-encrypting drives installed.
- Dell Enterprise Server v8.5 has been validated with VMware ESX/ESXi 5.5.

Resolved Technical Advisories v8.5

- If the iOS Web Clip URL policy value is specified after Enterprise Server installation and before all services are started, services now properly start. [DDPS-162]
- In the Policy Template Editor, the following PBA Authentication policies now display in the Global Settings list instead of under Self-Encrypting Drives: Non-Cached User Login Attempts Allowed, Cached User Login Attempts Allowed, and Self Help Question/Answer Attempts Allowed. [DDPS-166]
- Server migration no longer fails if the DeviceData table in the database contains a locale value of more than 12 characters. [DDPS-167]
- If the SQL database becomes unavailable, the Dell Core Server service now remains in the Running state. [DDPS-572]
- Searches for users in the Remote Management Console that include the wildcard character with other characters no longer return additional users in the results. [DDPS-810]
- Optimizations have been made to inventory processing and related logging. [DDPS-819, DDPS-887, DDPS-888, DDPS-945, DDPS-947]
- The Cloud Edition download page on the Japanese Dell Enterprise Server now correctly displays Japanese characters. [DDPS-845]
- The Remote Management Console License page now consistently displays the correct license count, usage, and availability. [DDPS-866]
- Self-encrypting drives (SEDs) now successfully activate against Dell Enterprise Server. Previously, in a few cases, SEDs did not activate as expected. [DDPS-867]
- When a Device Lease Period expires, all user leases associated with the device now expire. [DDPS-900]
- The Cloud Edition download page on Dell Enterprise Server now correctly displays the OS versions supported with Cloud Edition. [DDPS-908]
- Improvements have been made to device lease renewal after expiration of the Device Lease Period. [DDPS-949]
- Error handling following a failed Preboot Authentication attempt is improved. [DDPS-962]
- In the Portuguese Remote Management Console, the tool tip for the Inactivity Period for Device Lock policy now displays the correct value range. [DDPS-965]
- Several previously unlocalized AdminHelp topics are now localized. [DDPS-972]
- During an upgrade, a Domain Required message no longer displays when a domain is already configured. [DDPS-1154]

New Features and Functionality v8.3.1

- Amended 11/2014 - Windows Server 2012 R2 Standard is supported with Dell Enterprise Server.
- Database indexing improvements provide optimization of inventory and inventory processing. [DDPS-579]

Resolved Technical Advisories v8.3.1

- Performance is improved with clients running Dropbox, Box, and WebEx. [DDPS-57, DDPS-488, DDPS-547]
- Amended 11/2014 - Enterprise Server Admin Help now correctly states, in the Cloud Storage policies topic, that an interval of any length in minutes will be accepted by the Server for the Cloud Storage Server Polling Interval. [DDPS-462]
- Amended 11/2014 - Enterprise Server Admin Help now correctly states, in the Global Settings policies topic, that an unlimited number of attempts can be set for Non-Cached User Login Attempts Allowed under PBA Authentication. [DDPS-465]

- On Shielded computers with multiple users, when user policy is overridden, all users now receive correct user policies. [DDPS-603]
- Dell Manager v7.1 now successfully activates against Dell Enterprise Server. [DDPS-614]
- During database migration from v7.3 or v7.4, MAC user leases are now properly created. [DDPS-637]
- In Policy Template Editor, deleting a new template that was based on a default template no longer deletes the default template. [DDPS-673]

New Features and Functionality v8.3

- The Dell Identity Server is now embedded in the Enterprise Server installer and no longer must be manually created. It can be installed in conjunction with Enterprise Server or separately, using the Custom Installation option.
- Reliability is improved through performance optimizations, transfer of features previously present in the Document Store to the relational database, and removal of Document Store.

Resolved Technical Advisories v8.3

- When re-activating different users on the same endpoint, the endpoint now consistently receives all policy updates. [28088]
- When using the Recover Endpoint option, if the user enters an invalid host name into the Host Name field, an error message now displays and the user can correct the entry. Previously, an unhandled exception occurred, and the Remote Management Console became unresponsive. [DDPS-55]
- When provisioned by Exchange ActiveSync, iOS devices now move as expected from the Discovered to the Protected state on the Protection Status page. [DDPS-68]
- The Dell Compatibility Server and Dell Identity Server services now properly start after Enterprise Server installation and configuration are complete. [DDPS-85, DDPS-86]
- After an inventory update, in Portuguese and Brazilian Portuguese locales, Effective Policy now reflects the updated values. [DDPS-95]
- The list of CA certificates now includes all DoD certificates; all certificates are placed into the correct directories during installation; and self-signed certificates are properly created. [DDPS-111, DDPS-125, DDPS-131]
- When adding Endpoint Groups, the list of Endpoint Group members can now be previewed before the group is created. [DDPS-114, DDPS-122]
- On the Endpoint Search page, endpoints with the Hidden status are now indicated as Hidden rather than Visible in the Endpoint Visibility column. [DDPS-124]
- In the Japanese locale, Dell Compatibility Server, Dell Device Server, and Dell Identity Server services now properly start after installation and configuration. [DDPS-134]
- When an endpoint is renamed, duplicate entries for it no longer display on the Endpoint Search page. [DDPS-135]
- In the French locale, the Dell Compatibility Server service now properly starts after Enterprise Server installation and configuration are complete. [DDPS-147]
- In the French locale, policy values of "true" and "false" are now being correctly set and stored. [DDPS-153]
- The Compliance Reporter Pending Policy Report is now functioning properly. [DDPS-320]
- Migration to v8.x when using a Microsoft SQL 2005 database is improved, and policy is now decrypted by Windows Shield clients as expected. [DDPS-351]
- During installation of the front-end proxy components, the back-end Enterprise Server host name is now correctly set as entered during installation. [DDPS-353]
- After policy is enforced, the Applied Policy table in the database now displays the correct Device ID, regardless of whether the policy update included device policy. [DDPS-365]
- After policy is enforced, the applied policy is now properly truncated and displays the correct Date Enforced time stamp. [DDPS-376]
- After migration, locale information of Windows Shield clients are now correctly formatted. [DDPS-377]
- On the Endpoint Details page, Cloud Device Control commands now correctly display when an SED is activated. [DDPS-379]

Technical Advisories v8.3

- Some areas of the Remote Management Console are not fully localized. [DDPS-157]
- A short time after an iOS device acknowledges receipt of the Wipe Device command, its Current State may return to Discovered on the Endpoint Search page. [DDPS-163]
- The following Mobile - iOS Restrictions Policies are not enforced on iOS7 devices: Allow Assistant, Allow Installing Apps, Allow iTunes, Allow Screen Capture, and Allow YouTube. [DDPS-348]
- Recovery tools from pre-v8.3 Enterprise Servers cannot recover HCA-encrypted drives. To allow a pre-v8.3 Enterprise Server to recover v8.3 HCA-encrypted drives, an updated LSARecoveryLibDll.dll must be deployed to the pre-8.3 Enterprise Server.

Instructions:

1. At www.dell.com/support, search "HCA recovery" to find the knowledge base article associated with this issue. Download the attached ZIP file, which contains the updated LSARecoveryLibDll.dll.
2. Stop the Core Server, Security Server, and Console services.
3. Copy LSARecoveryLibDll.dll to the following components' installation directories: Core Server, Security Server, and Console.
4. Restart the Core Server, Security Server, and Console services.

[DDPS-468]

New Features and Functionality v8.1

- Enterprise managed smart cards for PBA Authentication is available as of v8.1.

Resolved Technical Advisories v8.1

- The certificate that is created or imported into the Server installer is now used for all components, not just the Dell Security Server.

Technical Advisories v8.1

- Adding enterprise managed smart cards in v8.1 requires the use of Certificate Revocation List (CRL) in AD. The Enterprise Server does not support binding to global catalogs (does not support binding to port 3268 for smart card authentication) for CRL distribution point resolution. The CRL distribution is not a global catalog replicated resource and the Enterprise Server cannot use the global catalog for CRL distribution point resolution. Configuration of individual domains in the Remote Management Console (in Domains > Add Domains) are required if enterprise managed smart cards will be used.

  If you intend to migrate your Enterprise Server or if you are already are using the global catalog as a mount point and want to use smart cards for PBA Authentication, contact Dell ProSupport for guidance.
- A Microsoft issue has caused Certificate Authorities installed on Windows Server 2012 that issue any of the certificates in a chain of trust used for smart card authentication to provide an invalid LDAP URL to the certificate's revocation list.

  Specifically, "A CA does not replace space characters in URL paths for CRL distribution points and authority information access extensions on a computer that is running Windows Server 2012".

  Microsoft has released a hotfix to correct this issue, which is available at http://support.microsoft.com/kb/2827759. Users will be required to enter an email address to which a link will be sent where the actual download will occur.

  This patch needs to be installed on any Windows Server 2012 CA that issues a certificate contained in the smart card's chain of trust. Once the hotfix is in place, the certificate service will need to be restarted and the affected certificates will need to be renewed or recreated in order to pick up the corrected LDAP URL.

New Features and Functionality v8.0

- Microsoft SQL Server 2012 Standard Edition / Business Intelligence / Enterprise Edition is now supported for the Enterprise Server database.
- The Policy Categories in the Remote Management Console have been renamed, as follows:
  - Shield for Windows has been renamed to Windows Encryption
  - Manager for SED has been renamed to Self-Encrypting Drives
  - Manager for BitLocker has been renamed to BitLocker
  - Shield for Mac has been renamed to Mac Encryption
  - Exchange Active Sync has been renamed to Mobile - EAS
  - iOS has been renamed to Mobile - iOS

Resolved Technical Advisories v8.0

- Forensic Mode is now automatically set by default in both the Security Server and Device Server. Forensic Mode is enabled on back-end servers and disabled on front-end servers. These settings are placed appropriately upon installation.
- Templates can now be applied only at the Enterprise level.
- Group priority settings in the Remote Management Console to control policy arbitration now work as expected.

Resolved Technical Advisories v7.7.2

- The issue of device policy revisions not being properly updated has been resolved. The Enterprise Server is now correctly sending the policy with the correct revision number to the encryption client.
- Occasional activation failures related to Document Store integration have been resolved.

Technical Advisories v7.7.2

- The list of reports does not display in Compliance Reporter when using Internet Explorer 10. To work around the issue, once at the Compliance Reporter web page, go to Internet Explorer's menu bar and select **Tools** > **Compatibility View settings**. When the Compatibility View Settings dialog displays, click Add and then click **Close**. The list of reports will now display as usual.

New Features and Functionality v7.7.1

- SkyDrive has been added to the protection providers list in the Enterprise Server in preparation for an upcoming client release that will enable the functionality.

Resolved Technical Advisories v7.7.1

- Overall improvements to the way Policy Proxy communicates with the Enterprise Server have been made in this release. As such, pre-v7.7.1 Policy Proxies are not compatible with v7.7.1 or later Enterprise Servers.
- The issue of the acknowledgment between the Policy Proxy and the Enterprise Server to retain users/Shields/devices in the Policy Active Lease table has been resolved.
- The empty Dell folder is now removed from the directory tree after uninstalling. [25291]

Technical Advisories v7.7.1

- An issue has been discovered where an individual is not inheriting groups admin rights. To work around the issue:

  Go to <Core Server install dir> and locate the *dotnetconnector.config* file.

  Change "localhost" to the FQDN of the server where Console Web Services is installed (usually the same server as the Core Server), such as:

  ServerHostName=QAtest.domain.com

New Features and Functionality v7.7

Dell Document Store

This release adds the Dell Document Store for high-performance caching for policy and staging for outgoing commands sent to the Dell Security Server and Dell Policy Proxy.

Dell Message Broker

This release adds the Dell Message Broker Service to optimize Dell Enterprise Server communications.

Dell Compliance Reporter

Two new fields have been added to the Dell Compliance Reporter's Device Details Report for up-to-date reporting capabilities when using Dell Data Protection | Mobile Edition.

Exchange ActiveSync Management

To enable Exchange ActiveSync management of mobile devices, two new components are available: *EAS Device Manager* - which enables over-the-air functionality and *EAS Mailbox Manager* - which is the Exchange mailbox agent. Both components are installed on the Exchange Server, enabling an enterprise to effectively manage Android and iOS devices. For more information, see the *Enterprise Server Installation and Migration Guide*.

Technical Advisories v7.2.3

- During certificate configuration for the Dell Compatibility Server components (java keystore) and the Dell Core Server (Microsoft keystore), if certificates are not generated or imported for all of these components, then the Dell Enterprise Server may not function correctly.
- If two certificates with the same name (same name = same subject or same CN) exist in the Microsoft keystore (for instance, one self-signed [signed by the Root Agency] and one signed by the domain), the Dell Core Server Service cannot start. Because the Dell Core Server is attempting to create a port associated to a certificate (for SSL), the name is ambiguous when there are multiple certificates with the same CN in the same keystore location (such as Personal/Certificates for the local computer). An "Error during server startup" message will be displayed in the Dell Core Server's output.log file. To work around this issue, use the MMC to remove one of the certificates, which removes the ambiguity.
- Compliance Reporter report names which include special characters fail to produce a report as expected. To work around this issue, do not use special characters in report names. [21836]
- If an administrator enters invalid alternate credentials in the Dell Server Configuration Tool (database initialization or database migration), an error displays, indicating invalid credentials were entered. In this case, initialization or migration will not run. To work around this issue, click Finish, restart the Dell Server Configuration Tool, and enter valid credentials. [21887]
- When a device is marked "removed", such as with the Lease Period Expiration policy, the device is not available in the Dell Enterprise Server for device recovery. To resolve this issue, in the AdminHelp, search keyword "EMS Recovery for User "Removed" from Database.". [22031]
- Compliance Reporter reports can only be deleted by a "reportadmin", even if the logged in user account is the "reportowner". To resolve this issue, either log in as "reportadmin" or ask your Compliance Reporter report administrator to delete the report. [22088]

Technical Advisories v7.2.1

- No known Enterprise Server issues.

Technical Advisories v7.2

- No known Enterprise Server issues.

Technical Advisories v7.0/7.0.1

- If installing the Dell Enterprise Server and its components on non-default ports, the Dell Enterprise Server installer does not check for conflicting ports. To workaround this issue, ensure that each port entry is unique.

2

Default Policy Changes

Default policy value changes in new Dell Server versions do not affect Server migrations. This prevents unexpected changes to existing environments. If you need to apply the new default values, you must manually change and commit the policy after migration is complete.

CAUTION: Carefully plan changes to default policy values, taking into account their effects on all groups, endpoints, or users to which the policy applies.

Global Settings Default Policy Changes

The following Global Settings policies' default values are changed.

Table 1. Security Management Server or Security Management Server Virtual v9.8 - Global Settings Default Policy Value Changes

Technology Group	Policy	Previous Default Value	New Default Value
Global Settings	Custom Support Dialog	\"Dell listens to customers and delivers worldwide innovative technology, business solutions and services they trust and value.\nFor more information, visit us online\n\nTechnical Support: Online Support\n\nProduct Questions and Sales:\nIn the US? Call 877.459.7304 Ext. 4310039\nInternational Support? Find the appropriate number here.\"	For questions or concerns with Dell Data Security, contact your system administrator or help desk.

Data Guardian Default Policy Changes

The following Data Guardian policies' default values are changed.

Table 2. Security Management Server or Security Management Server Virtual v9.8 - Data Guardian Default Policy Value Changes

Technology Group	Policy	Previous Default Value	New Default Value
Data Guardian	No policies' default values changed in v9.8.	Not applicable	Not applicable

Table 3. Enterprise Server or VE v9.7 - Data Guardian Default Policy Value Changes

Technology Group	Policy	Previous Default Value	New Default Value
Data Guardian	Enable Callback Beacon	Selected	Not Selected

Endpoint Security Suite Enterprise Default Policy Changes

The following Endpoint Security Suite Enterprise policies' default values are changed.

Table 4. Security Management Server or Security Management Server Virtual v9.8 - Endpoint Security Suite Enterprise policy changes

Technology Group	Policy	Previous Default Value	New Default Value
Advanced Threat Prevention	No policies' default values changed in v9.8.	Not applicable	Not applicable

Table 5. Enterprise Server or VE 9.7 - Endpoint Security Suite Enterprise policy changes

Technology Group	Policy	Previous Default Value	New Default Value
Advanced Threat Prevention	Memory Actions - Exclude Executable Files	\Windows \System32\CmgShieldService.exe \Windows\System32\EMSService.exe	\Windows \System32\CmgShieldService.exe \Windows\System32\EMSService.exe \Program Files\Dell\Dell Data Protection \Threat Protection\DellAVAgent.exe \Program Files\McAfee\Agent \cmdagent.exe \Program Files\McAfee\Agent \FrmInst.exe \Program Files\McAfee\Agent \macmnsvc.exe \Program Files\McAfee\Agent \macompatsvc.exe \Program Files\McAfee\Agent \maconfig.exe \Program Files\McAfee\Agent\masvc.exe \Program Files\McAfee\Agent \x86\FrmInst.exe \Program Files\McAfee\Agent \x86\macompatsvc.exe \Program Files\McAfee\Agent \x86\marepomirror.exe \Program Files\McAfee\Agent \x86\McScanCheck.exe \Program Files\McAfee\Agent \x86\McScript_InUse.exe \Program Files\McAfee\Agent \x86\mctray_back.exe \Program Files\McAfee\Agent \x86\Mue.exe \Program Files\McAfee\Agent \x86\policyupgrade.exe \Program Files\McAfee\Agent \x86\UpdaterUI.exe

Table 5. Enterprise Server or VE 9.7 - Endpoint Security Suite Enterprise policy changes

Technology Group	Policy	Previous Default Value	New Default Value
			\Program Files\McAfee\Endpoint Security \Endpoint Security Platform \ESConfigTool.exe \Program Files\McAfee\Endpoint Security \Endpoint Security Platform \MFEConsole.exe \Program Files\McAfee\Endpoint Security \Endpoint Security Platform\mfeesp.exe \Program Files\McAfee\Endpoint Security \Endpoint Security Platform \mfeProvisionModeUtility.exe \Program Files\McAfee\Endpoint Security \Endpoint Security Platform \PwdUninstall.exe \Program Files\McAfee\Endpoint Security \Endpoint Security Platform\RepairCache \CCUninst.exe \Program Files\McAfee\Endpoint Security \Endpoint Security Platform\RepairCache \McAfee_Common_x64.exe \Program Files\McAfee\Endpoint Security \Endpoint Security Platform\RepairCache \McAfee_Common_x64.msi \Program Files\McAfee\Endpoint Security \Endpoint Security Platform\RepairCache \McAfee_Common_x86.msi \Program Files\McAfee\Endpoint Security \Endpoint Security Platform\RepairCache \setupCC.exe \Program Files\McAfee\Endpoint Security \Endpoint Security Platform \VSCore_ENS_10.1\Release\aacinfo.exe \Program Files\McAfee\Endpoint Security \Endpoint Security Platform \VSCore_ENS_10.1\Release \cacheinfo.exe \Program Files\McAfee\Endpoint Security \Endpoint Security Platform \VSCore_ENS_10.1\Release\fwinfo.exe \Program Files\McAfee\Endpoint Security \Endpoint Security Platform \VSCore_ENS_10.1\Release \mfecanary.exe \Program Files\McAfee\Endpoint Security \Endpoint Security Platform \VSCore_ENS_10.1\Release\mfefire.exe \Program Files\McAfee\Endpoint Security \Endpoint Security Platform \VSCore_ENS_10.1\Release\mfehidin.exe \Program Files\McAfee\Endpoint Security \Endpoint Security Platform \VSCore_ENS_10.1\Release\mfemms.exe

Table 5. Enterprise Server or VE 9.7 - Endpoint Security Suite Enterprise policy changes

Technology Group	Policy	Previous Default Value	New Default Value
			\Program Files\McAfee\Endpoint Security \Endpoint Security Platform \VSCore_ENS_10.1\Release\mfevtps.exe \Program Files\McAfee\Endpoint Security \Endpoint Security Platform \VSCore_ENS_10.1\Release\mmsinfo.exe \Program Files\McAfee\Endpoint Security \Endpoint Security Platform \VSCore_ENS_10.1\Release\vtpinfo.exe \Program Files\McAfee\Endpoint Security \Endpoint Security Platform \VSCore_ENS_10.1\x64\aacinfo.exe \Program Files\McAfee\Endpoint Security \Endpoint Security Platform \VSCore_ENS_10.1\x64\cacheinfo.exe \Program Files\McAfee\Endpoint Security \Endpoint Security Platform \VSCore_ENS_10.1\x64\fwinfo.exe \Program Files\McAfee\Endpoint Security \Endpoint Security Platform \VSCore_ENS_10.1\x64\mfecanary.exe \Program Files\McAfee\Endpoint Security \Endpoint Security Platform \VSCore_ENS_10.1\x64\mfefire.exe \Program Files\McAfee\Endpoint Security \Endpoint Security Platform \VSCore_ENS_10.1\x64\mfehidin.exe \Program Files\McAfee\Endpoint Security \Endpoint Security Platform \VSCore_ENS_10.1\x64\mfemms.exe \Program Files\McAfee\Endpoint Security \Endpoint Security Platform \VSCore_ENS_10.1\x64\mfevtps.exe \Program Files\McAfee\Endpoint Security \Endpoint Security Platform \VSCore_ENS_10.1\x64\mmsinfo.exe \Program Files\McAfee\Endpoint Security \Endpoint Security Platform \VSCore_ENS_10.1\x64\vtpinfo.exe \Program Files\McAfee\Endpoint Security \Firewall\FWInstCheck.exe \Program Files\McAfee\Endpoint Security \Firewall\FwWindowsFirewallHandler.exe \Program Files\McAfee\Endpoint Security \Firewall\mfefw.exe \Program Files\McAfee\Endpoint Security \Firewall\RepairCache \McAfee_Firewall_x64.msi \Program Files\McAfee\Endpoint Security \Firewall\RepairCache \McAfee_Firewall_x86.msi

Table 5. Enterprise Server or VE 9.7 - Endpoint Security Suite Enterprise policy changes

Technology Group	Policy	Previous Default Value	New Default Value
			\Program Files\McAfee\Endpoint Security \Firewall\RepairCache\setupFW.exe \Program Files\McAfee\Endpoint Security \Web Control\McChHost.exe \Program Files\McAfee\Endpoint Security \Web Control\mfewc.exe \Program Files\McAfee\Endpoint Security \Web Control\mfewch.exe \Program Files\McAfee\Endpoint Security \Web Control\mfewcui.exe \Program Files\McAfee\Endpoint Security \Web Control\RepairCache \McAfee_Web_Control_x86.msi \Program Files\McAfee\Endpoint Security \Web Control\RepairCache\setupWC.exe \Program Files\McAfee\marepomirror.exe \Program Files\McAfee \McScanCheck.exe \Program Files\McAfee \McScript_InUse.exe \Program Files\McAfee\mctray_back.exe \Program Files\McAfee\Mue.exe \Program Files\McAfee \policyupgrade.exe \Program Files\McAfee\UpdaterUI.exe \Program Files (x86)\McAfee\Endpoint Security\Endpoint Security Platform \MaComServer.exe \Program Files (x86)\McAfee\Endpoint Security\Endpoint Security Platform \MFEConsole.exe \Program Files (x86)\McAfee\Endpoint Security\Endpoint Security Platform \mfeProvisionModeUtility.exe \Program Files (x86)\McAfee\Endpoint Security\Endpoint Security Platform \RepairCache\CCUninst.exe \Program Files (x86)\McAfee\Endpoint Security\Endpoint Security Platform \VSCore_ENS_10.1\Release\aacinfo.exe \Program Files (x86)\McAfee\Endpoint Security\Endpoint Security Platform \VSCore_ENS_10.1\Release \cacheinfo.exe \Program Files (x86)\McAfee\Endpoint Security\Endpoint Security Platform \VSCore_ENS_10.1\Release\fwinfo.exe \Program Files (x86)\McAfee\Endpoint Security\Endpoint Security Platform

Table 5. Enterprise Server or VE 9.7 - Endpoint Security Suite Enterprise policy changes

Technology Group	Policy	Previous Default Value	New Default Value
			\VSCore_ENS_10.1\Release \mfecanary.exe \Program Files (x86)\McAfee\Endpoint Security\Endpoint Security Platform \VSCore_ENS_10.1\Release\mfefire.exe \Program Files (x86)\McAfee\Endpoint Security\Endpoint Security Platform \VSCore_ENS_10.1\Release\mfehidin.exe \Program Files (x86)\McAfee\Endpoint Security\Endpoint Security Platform \VSCore_ENS_10.1\Release\mfemms.exe \Program Files (x86)\McAfee\Endpoint Security\Endpoint Security Platform \VSCore_ENS_10.1\Release\mfevtps.exe \Program Files (x86)\McAfee\Endpoint Security\Endpoint Security Platform \VSCore_ENS_10.1\Release\mmsinfo.exe \Program Files (x86)\McAfee\Endpoint Security\Endpoint Security Platform \VSCore_ENS_10.1\Release\vtpinfo.exe \Program Files (x86)\McAfee\Endpoint Security\Endpoint Security Platform \VSCore_ENS_10.1\x64\aacinfo.exe \Program Files (x86)\McAfee\Endpoint Security\Endpoint Security Platform \VSCore_ENS_10.1\x64\cacheinfo.exe \Program Files (x86)\McAfee\Endpoint Security\Endpoint Security Platform \VSCore_ENS_10.1\x64\fwinfo.exe \Program Files (x86)\McAfee\Endpoint Security\Endpoint Security Platform \VSCore_ENS_10.1\x64\mfecanary.exe \Program Files (x86)\McAfee\Endpoint Security\Endpoint Security Platform \VSCore_ENS_10.1\x64\mfefire.exe \Program Files (x86)\McAfee\Endpoint Security\Endpoint Security Platform \VSCore_ENS_10.1\x64\mfehidin.exe \Program Files (x86)\McAfee\Endpoint Security\Endpoint Security Platform \VSCore_ENS_10.1\x64\mfemms.exe \Program Files (x86)\McAfee\Endpoint Security\Endpoint Security Platform \VSCore_ENS_10.1\x64\mfevtps.exe \Program Files (x86)\McAfee\Endpoint Security\Endpoint Security Platform \VSCore_ENS_10.1\x64\mmsinfo.exe \Program Files (x86)\McAfee\Endpoint Security\Endpoint Security Platform \VSCore_ENS_10.1\x64\vtpinfo.exe

Table 5. Enterprise Server or VE 9.7 - Endpoint Security Suite Enterprise policy changes

Technology Group	Policy	Previous Default Value	New Default Value
			\Program Files (x86)\McAfee\Endpoint Security\Web Control\McChHost.exe \Program Files (x86)\McAfee\Endpoint Security\Web Control\mfewc.exe \Program Files (x86)\McAfee\Endpoint Security\Web Control\mfewch.exe \Program Files (x86)\McAfee\Endpoint Security\Web Control\mfewcui.exe \Program Files (x86)\McAfee\Endpoint Security\Web Control\RepairCache \McAfee_Web_Control_x64.msi \Program Files (x86)\McAfee\Endpoint Security\Web Control\RepairCache \setupWC.exe \Program Files (x86)\McAfee\Endpoint Security\Web Control\x64\mfewch.exe \Windows\System32\mfevtps.exe \Program Files\McAfee\Endpoint Security \Endpoint Security Platform \LogDebugSetter.exe \Program Files\McAfee\Endpoint Security \MfeUpgradeTool.exe